



# Performance and Accountability Report

Fiscal Year 2006



Homeland  
Security



# Homeland Security

Additional copies of the Department of Homeland Security's Performance and Accountability Report for Fiscal Year 2006 are available by writing to:

U.S. Department of Homeland Security  
Office of the Chief Financial Officer  
Program Analysis and Evaluation  
Washington, DC 20528

Or by phone, fax or email at:  
(202) 447-5145 or 5146 (Phone)  
(202) 447-5144 (Fax)  
PAR@dhs.gov

Electronic versions may be accessed and downloaded via the DHS public website at <http://www.dhs.gov/xabout>

## Message from the Secretary

November 15, 2006



I am pleased to provide the Department of Homeland Security's Performance and Accountability Report for fiscal year 2006. The report provides a clear view of the Department's achievements under focused goals to preserve our freedoms and protect our homeland.

For almost four years now, the Department of Homeland Security has led a national effort to protect our country and our citizens from terrorist and natural threats. Realizing that we can reduce risk, but not completely eliminate it, we pursued our goals with a sense of urgency and daily diligence to minimize risk and ensure our nation can respond and recover quickly should an incident occur.

First, our goals optimize our security, but not security at any price. Our security strategy promotes Americans' freedom, privacy, prosperity, and mobility. Second, our goals drive continuous improvement as terrorists will not relent, and natural disasters are inevitable. Third, we must be an effective steward of public resources – setting and meeting priorities, sound financial management, a commitment to measure and report performance, and fostering innovation. Finally, our work must be guided by the understanding that effective security is built upon a network of systems that spans all levels of government

and the private sector. DHS does not, and should not, own or control all of these systems. We set a clear national strategy and design an architecture in which separate roles and responsibilities for security are fully integrated among public and private stakeholders. We draw on the strength of our network of partners and assets, functioning as seamlessly as possible with state and local leadership, first responders, the private sector, our international partners, and, most certainly, the general public.

This report provides detailed accomplishments of 2006. Some of the highlights include:

- Although over 600 million people fly each year, the Transportation Security Administration was able to perform necessary passenger screening operations preventing and protecting against adverse actions while attaining a new high in customer satisfaction. Customer Satisfaction reached 81%, a new high for screening operations at the nation's security checkpoints.
- Almost 7 million cargo containers arrive and are offloaded at U.S. seaports each year. The U.S. Customs and Border Protection increased the percent of shipping containers processed through its Container Security Initiative prior to entering U.S. ports from 48% in FY 2004 to 82% in FY 2006. This significantly decreases the risk of terrorist materials entering our country while providing processes to facilitate the flow of safe and legitimate trade and travel from more foreign ports.
- 185,944 aliens illegally in the United States were removed by U.S. Immigration and Customs Enforcement pursuant to an immigration judge issuing an order for removal. In FY 2006 the quarterly ratio of removals to orders increased from 109% last year to an estimated 124% this year. Illegal aliens are being removed in accordance with orders more rapidly than in the past.
- In a major initiative of the Secure Border Initiative, the Department ended the practice of "catch and release" along the southern and northern border. In the past we apprehended illegal aliens from countries other than Mexico and then released them on their own recognizance. Often these illegal aliens failed to return for their hearing. Ending this practice and replacing it with "catch and return" is a breakthrough in deterring illegal immigration on the southern border. Last year, DHS detained 34 percent of non-Mexican illegal aliens apprehended along the southern border. Currently 99 percent are being detained.

- 51,249 individuals were trained by the Federal Law Enforcement Training Center, providing them skills needed to perform law enforcement duties helping secure our nation.
- \$485 million in competitive grants were provided to fire departments and emergency responders to strengthen the Nation's overall level of preparedness and ability to respond to fire and fire related hazards.
- The five-year average number of chemical spills and oil spills greater than 100 gallons declined 11.9% from the FY 2005 level, indicating continuing improved performance of the U.S. Coast Guard in preventing discharges of chemicals or oil into U.S. navigable waters.
- The President, Vice President, visiting world leaders and other protectees of the U.S. Secret Service arrived and departed safely 100% of the time at more than 6,275 travel stops. The Secret Service continues to perform flawlessly by protecting our key national leaders without incident ensuring our top elected officials can perform the duties of their office.
- More than 6 million applications were processed by the U.S. Citizenship and Immigration Services which also conducted the naturalization of approximately half a million new citizens.

These front line results are backed by efforts to improve the Department overall. The President's Management Agenda continues to guide efforts to make programs more efficient, effective and results-oriented. Work remains to fully meet all standards of the President's agenda which becomes more stringent each year. This year's report again discusses how we are fulfilling the President's Management Agenda.

This report identifies material internal control weaknesses and actions the agency is taking to resolve them. My assurance statements and information related to the Federal Managers' Financial Integrity Act's Section 2 and Section 4, the Department of Homeland Security Financial Accountability Act, as well as an assessment of financial and performance data completeness and reliability, are provided in the Management Assurances section of this report.

Moving forward together with our partners and the public, we will continue building upon our successful foundation over nearly four years at Homeland Security. We will proceed with unyielding focus and determination.

Sincerely,

A handwritten signature in black ink, appearing to read 'Michael Chertoff', with a long horizontal stroke extending to the right.

Michael Chertoff



# Table of Contents

Message from the Secretary .....	1
Table of Contents .....	3
About the Fiscal Year 2006 Performance and Accountability Report .....	4
SECTION I. MANAGEMENT'S DISCUSSION & ANALYSIS .....	5
Mission and Organizational Structure .....	6
Performance Highlights: Goals, Objectives, and Results .....	9
Secretary's Management Assurances .....	51
Independent Auditors' Report on DHS' FY 2006 Internal Controls over Financial Reporting .....	53
Other Management Information, Initiatives, and Issues .....	72
Limitations of the Financial Statements .....	76
SECTION II. PERFORMANCE INFORMATION .....	77
Introduction .....	78
Completeness and Reliability .....	79
Strategic Goal 1 – Awareness .....	83
Strategic Goal 2 – Prevention .....	85
Strategic Goal 3 – Protection .....	120
Strategic Goal 4 – Response .....	138
Strategic Goal 5 – Recovery .....	142
Strategic Goal 6 – Service .....	144
Strategic Goal 7 – Organizational Excellence .....	150
Fiscal Year 2005 Estimated Actuals Updates .....	154
Program Evaluations .....	156
SECTION III. FINANCIAL INFORMATION .....	177
Message from the Chief Financial Officer .....	178
Independent Auditor's Report .....	179
Introduction .....	247
Balance Sheets .....	248
Statements of Net Cost .....	250
Statements of Changes in Net Position .....	252
Statements of Budgetary Resources .....	253
Statements of Financing .....	255
Statements of Custodial Activity .....	257
Notes to the Financial Statements (Unaudited) .....	258
SECTION IV - OTHER ACCOMPANYING INFORMATION .....	319
Tax Burden / Tax Gap .....	320
Improper Payments Information Act (IPIA) Reporting Details .....	320
Major Management Challenges Facing the Department of Homeland Security .....	328
Management's Response to the Office of the Inspector General's Report on Major Management Challenges Facing the Department of Homeland Security .....	347
Effects of Hurricanes Katrina and Rita .....	367
SECTION V. APPENDICES .....	371
Appendix A – References and Resources .....	372
Appendix B – List of Department Websites .....	373
Appendix C – Glossary of Acronyms and Abbreviations .....	374

# ABOUT THE FISCAL YEAR 2006 PERFORMANCE AND ACCOUNTABILITY REPORT

This report, prepared in accordance with the Reports Consolidation Act of 2000, presents the results of the Department of Homeland Security's (DHS) program and financial performance for FY 2006. It is divided into sections:

The **Secretary's Message** provides the Secretary's perspective of the Department's progress during FY 2006.

The **Management's Discussion and Analysis (MD&A)** section explains the Department's mission, goals and organization, summarizes program and financial performance, and addresses major management challenges. The MD&A also reports progress in implementing the President's Management Agenda.

The **Performance Section** assesses progress in achieving the Department's goals as presented in the Strategic Plan and Performance Budget for FY 2006.

The **Financial Section** demonstrates our commitment to effective stewardship over the funds DHS receives to carry out the mission of the Department, including compliance with relevant financial management legislation. It includes the **Independent Auditor's Report**, an independent opinion on the Financial Statements provided by the Department's Office of Inspector General (OIG), and provides the Department's **Annual Financial Statements**.

The **Other Accompanying Information** section contains the Inspector General's (IG) report on Major Management Challenges followed by the Department's response to the challenges. This section also contains information on Improper Payments and the effects of Hurricanes Katrina and Rita.

In addition, the **Appendices** contain a list of references and resources, a list of Department web sites and a glossary of acronyms and abbreviations.

This report satisfies the reporting requirements of the following laws:

- Federal Managers' Financial Integrity Act of 1982;
- Government Performance and Results Act of 1993;
- Government Management Reform Act of 1994;
- Clinger-Cohen Act of 1996;
- Reports Consolidation Act of 2000;
- Federal Information Security Management Act of 2002;
- Chief Financial Officer Act of 1990; and
- Department of Homeland Security Financial Accountability Act of 2004.



# Management's Discussion and Analysis

Part I

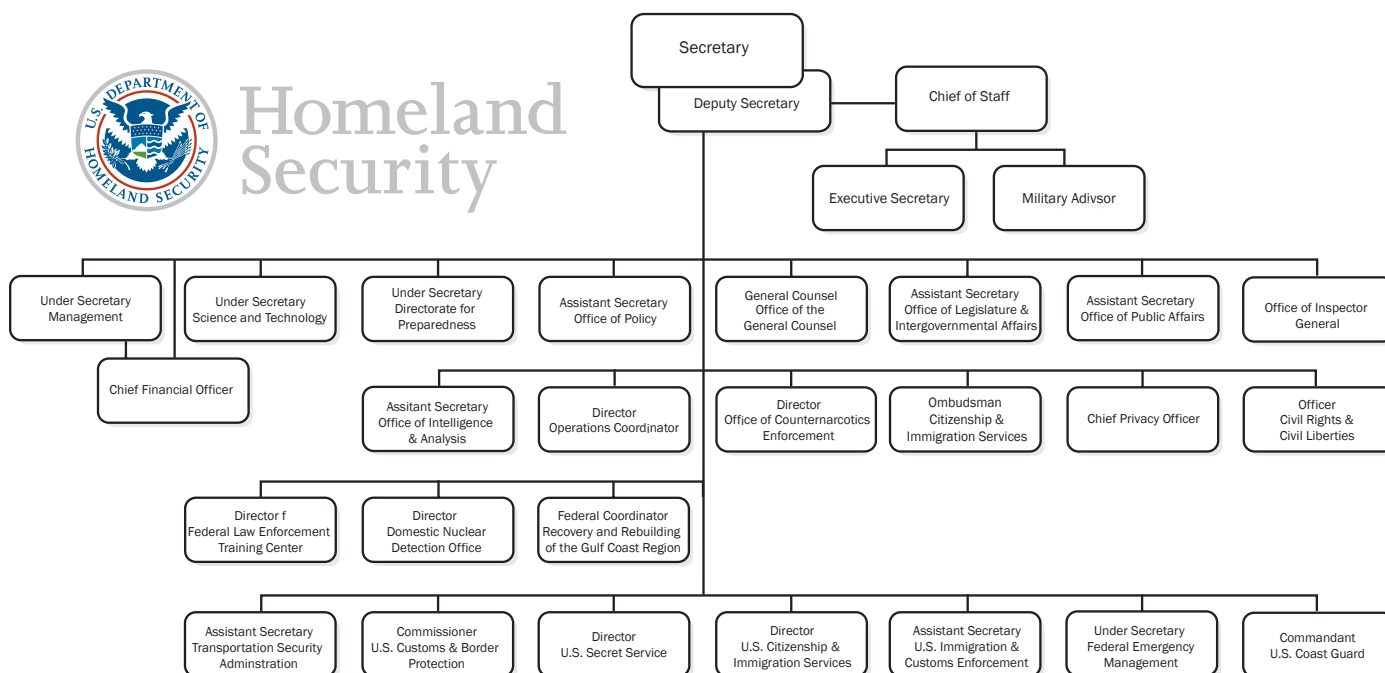
## Mission and Organizational Structure

**T**he U.S. Department of Homeland Security is a cabinet-level agency of the Executive Branch of the Federal government, responsible for leading the unified national effort to secure America. Our mission gave us focus for the year:

***Preserving our freedoms, protecting America... We secure our homeland***

DHS leverages resources within Federal, state, and local governments, coordinating the transition of multiple agencies and programs into a single, integrated agency focused on protecting the American people and their homeland. More than 87,000 different governmental jurisdictions at the Federal, state, and local level have homeland security responsibilities. The comprehensive national strategy develops a complementary system connecting all levels of government without duplicating effort. Homeland Security is truly a “national mission.”

To accomplish the mission, in Fiscal Year 2006 the Department was organized as shown below.



NOTE: The FY 2007 Homeland Security Appropriations Bill references an integration of the Federal Emergency Management Agency (FEMA) and the Preparedness Directorate. This change was not in effect in FY 2006.



## DEPARTMENT COMPONENTS

**T**he following list contains the major components that make up the Department of Homeland Security.

The **Office of the Secretary** oversees activities with other Federal, state, local, and private entities as part of a collaborative effort to strengthen our borders, provide for intelligence analysis and infrastructure protection, improve the use of science and technology to counter weapons of mass destruction, and to create a comprehensive response and recovery system. The Office of the Secretary includes multiple offices that contribute to the overall Homeland Security mission.

The **Science and Technology Directorate** is the primary research and development arm of the Department. It provides Federal, state and local officials with the technology and capabilities to protect the homeland.

The **Preparedness Directorate** works with state, local, and private sector partners to identify threats, determine vulnerabilities, and target resources where risk is greatest, thereby safeguarding our borders, seaports, bridges and highways, and critical information systems.

The **Management Directorate** is responsible for procurement; human resources, information technology systems, facilities and equipment, and the identification and tracking of performance measurements.

The **Office of Chief Financial Officer** provides guidance and oversight of the Department's budget, financial management, and investment review functions to ensure funds necessary to carry out the Department's mission are obtained, allocated, and expended in accordance with the Department's priorities and relevant law and policies.

The **Office of Policy** is the primary policy formulation and coordination component for the Department of Homeland Security. It provides a centralized, coordinated focus to the development of Department-wide, long-range planning to protect the United States.

The **Office of Intelligence and Analysis** is responsible for using information and intelligence from multiple sources to identify and assess current and future threats to the United States.

The **Office of Operations Coordination** is responsible for monitoring the security of the United States on a daily basis and coordinating activities within the Department and with governors, Homeland Security Advisors, law enforcement partners, and critical infrastructure operators in all 50 states and more than 50 major urban areas nationwide.

The **Domestic Nuclear Detection Office** works to enhance the nuclear detection efforts of Federal, state, territorial, tribal, and local governments, and the private sector and to ensure a coordinated response to such threats.

The **Transportation Security Administration** protects the nation's transportation systems to ensure freedom of movement for people and commerce.

**United States Customs and Border Protection** is responsible for protecting our nation's borders in order to prevent terrorists and terrorist weapons from entering the United States, while facilitating the flow of legitimate trade and travel.

The **United States Secret Service** protects the President and other high-level officials and investigates counterfeiting and other financial crimes, including financial institution fraud, identity theft, computer fraud; and computer-based attacks on our nation's financial, banking, and telecommunications infrastructure.

The **Federal Law Enforcement Training Center** provides career-long training to law enforcement professionals to help them fulfill their responsibilities safely and proficiently.

**United States Citizenship and Immigration Services** is responsible for the administration of immigration and naturalization adjudication functions and establishing immigration services policies and priorities.

**United States Immigration and Customs Enforcement (ICE)** enforces Federal immigration and customs laws as the largest investigative arm of the Department of Homeland Security. ICE identifies criminal activities and eliminates vulnerabilities that threaten national security.

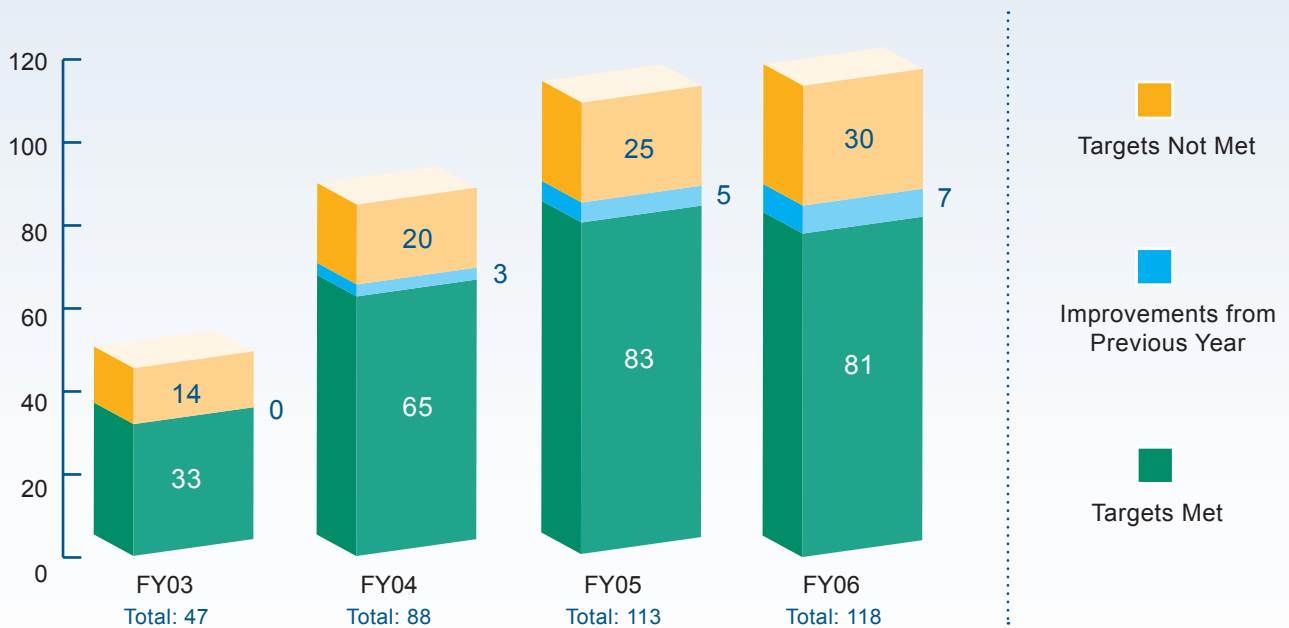
The **Federal Emergency Management Agency** prepares the nation for hazards, manages Federal response and recovery efforts following any national incident, and administers the National Flood Insurance Program.

The **United States Coast Guard** protects the public, the environment, and U.S. economic interests in the nation's ports and waterways, along the coast, on international waters, or in any maritime region as required to support national security.

## PERFORMANCE HIGHLIGHTS: GOALS, OBJECTIVES, AND RESULTS

The Department of Homeland Security (DHS) measures success in achieving its mission. The DHS strategic plan identifies strategic goals with objectives to achieve. DHS programs accomplish the objectives and establish performance goals with annual targets to measure progress. We established 118 specific target levels of performance under our program goals in fiscal year 2006. Each year we strive to make our targets more aggressive. During fiscal year 2006, 81 or 68.6%, of established performance measures met their target. Of those not met, there were seven (7) performance measures that did improve over their FY 2005 actuals. Details concerning our performance as compared with targets may be found in Section II, Performance Information. The following graph depicts the 4-year trend in meeting performance targets Department-wide.

### DEPARTMENT OF HOMELAND SECURITY PERFORMANCE TRENDS



The following areas of this section present highlights for each of the Department's seven strategic goals and their objectives. They identify program performance goals associated with each objective, and provide cost information along with an assessment of our performance during FY 2006. Detailed data concerning our performance is provided in Section II, Performance Information.

The seven DHS Strategic Goals are:

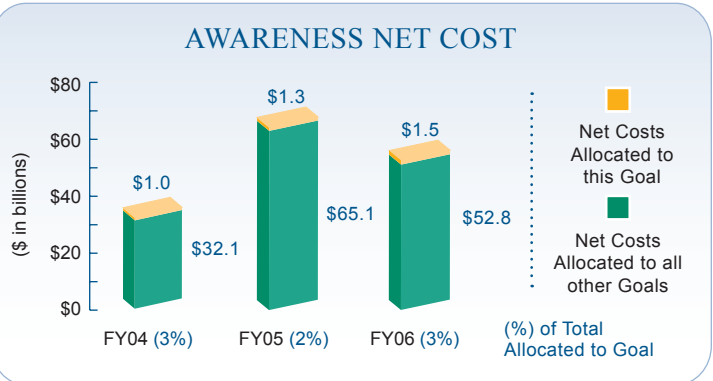
- 1. Awareness** - Identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and the American public.
- 2. Prevention** - Detect, deter and mitigate threats to our homeland.
- 3. Protection** - Safeguard our people and their freedoms, critical infrastructure, property and the economy of our nation from acts of terrorism, natural disasters or other emergencies.
- 4. Response** - Lead, manage and coordinate the national response to acts of terrorism, natural disasters or other emergencies.
- 5. Recovery** - Lead national, state, local and private-sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters or other emergencies.
- 6. Service** - Serve the public effectively by facilitating lawful trade, travel and immigration.
- 7. Organizational Excellence** - Value our most important resource - our people. Create a culture that promotes a common identity, innovation, mutual respect, accountability and teamwork to achieve efficiencies, effectiveness and operational synergies.



## Performance Results by Strategic Goal

### Strategic Goal 1 Awareness

Identify and understand threats, assess vulnerabilities, determine potential impacts and disseminate timely information to our homeland security partners and the American public.



### Public

erating Picture is a tool that  
ased our situational awareness  
ment, supporting responses to  
st, the California levy threat,  
dents. Supported by the  
ormation Network the Com-  
enables Federal agencies and  
s to operate collaboratively  
ation. The Common Operating  
mplemented nationwide for all  
ners, for all hazards, and for

**T**o fully support this strategic goal, we developed subordinate strategic objectives with supporting performance goals for programs. For each performance goal, we developed quantitative performance measures. Collectively, these measures assess progress in attainment of our strategic goal of Awareness.

The table below correlates our strategic objectives with the performance goals established for each objective, indicated by an objective number in the left hand column. The chart also indicates the estimated net cost of efforts to achieve the objective.

STRATEGIC GOAL 1 - AWARENESS				
STRATEGIC OBJECTIVES SUPPORTING GOAL 1				FY 06 Net Cost (in millions)
1.1 Gather, fuse, and analyze all terrorism and threat related intelligence.				\$ 168.1
1.2 Identify and assess the vulnerability of critical infrastructure and key assets.				\$ 56.8
1.3 Provide timely, actionable, accurate, and relevant information based on intelligence analysis and vulnerability assessments to homeland security partners, including the public.				\$ 127.0
1.4 Develop a Common Operating Picture for domestic situational awareness, including air, land, and sea.				\$ 862.8
<b>PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES</b>				<b>Detail on Page</b>
		1.3	Deter, detect, and prevent terrorist incidents by sharing domestic situational awareness through national operational communications and intelligence analysis. (Analysis and Operations)	83
1.1			100 percent distribution of sensitive threat information relative to Department of Homeland Security / Transportation Security Administration components, field elements and stakeholders. (Intelligence)	84
		1.3	Prevent known or suspected terrorists from gaining access to sensitive areas of the transportation system. (Transportation Vetting and Credentialing)	84
1.2			Protect the Nations high risk and most valued critical infrastructure and key resources (CI/KR) by characterizing and prioritizing assets, modeling and planning protective actions, building partnerships, and issuing targeted infrastructure protection grants. (Infrastructure Protection)	125

NOTE 1: The Net Cost measures the cost of supporting that entire strategic objective, not just the performance goal(s) identified in the table.

NOTE 2: Programs whose primary contribution is to this Strategic Objective are reported in this table. Strategic Objective 1.4 is supported by other Programs whose primary contribution is to other Strategic Objectives.

NOTE 3: Net Costs for a strategic objective do not directly correlate with the budget because many capabilities funded in the budget address multiple strategic objectives and because of the differences in how budgeting (obligational accounting) and accrual accounting allocate costs.

## HIGHLIGHTS

Some of the key performance measures used to gauge success in achieving the goal of Awareness are highlighted below. These measures illustrate some of our significant accomplishments during FY 2006 in achieving Awareness goals and objectives.

The Department of Homeland Security uses a risk-based approach to identify preventive and protective steps that increase security, and in turn, reduces the risk of harm to the Homeland. A quantifiable overall measurement of risk reduction would

be an ideal measure; however, there is not a straightforward way of calculating total risk reduction to all aspects of our Homeland at this time. Yet, the measure below shows the Department's progress in addressing risk reduction by increasing Awareness.

- **Improve real-time homeland security information and situational awareness through sharing and collaboration.**

Measure: *Percent of Federal, State and local agencies that maintain connectivity with the Homeland Security Operations Center (HSOC) via Homeland Security Information Network (HSIN) and participate in information sharing and collaboration concerning infrastructure status, potential threat and incident management information.* (Target Not Met) (See Page 83)

The HSOC serves as the nation's nerve center for information sharing and domestic incident management - dramatically increasing the vertical coordination between Federal, state, territorial, tribal, local, and private sector partners. Our ability to gather, analyze and disseminate information in a timely manner is key to successfully defending our homeland. The HSOC provides critical information to those who need it to prevent terrorist attacks, reduce vulnerability to attacks and disastrous acts of nature, minimize the damage to critical infrastructure, and assist in the response and recovery from such incidents. Although we did not meet our target, we made significant progress over FY 2005 results and will continue to set high targets for achievement.

- In addition, DHS activated in May 2006, the Common Operating Picture (COP) which is a display of relevant information that is derived from a Common Operating Database (COD) and shared by several agencies and organizations. The COP/COD system is a situational awareness tool that can be modified for the strategic, operational and tactical levels and is active in the National Operations Center. As part of an incrementally phased development effort, the Department's COP/COD system initially focused on the 2006 hurricane season and has been implemented in selected Department offices and inter-agency operation centers.

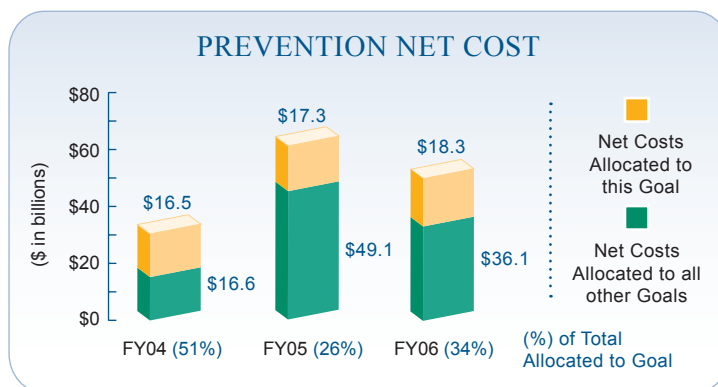
## FUTURE STEPS

**T**errorist threats to the nation will not only continue into the future, but also will become increasingly sophisticated. As the nation takes steps to harden potential targets, terrorists will look to exploit other vulnerabilities inherent to an open society. A key to preventing terrorist activity is the ability to act on accurate and timely information. The Department will continue building an integrated, comprehensive intelligence and warning system to detect terrorist activity before an attack occurs so pre-emptive, preventive and protective actions can be taken. The Homeland Security Information Network (HSIN) will be expanded to additional jurisdictions to provide operational information and communications pertaining to domestic incident management. The Department will form a National Operations Center, consolidating functions from the Homeland Security Operations Center, the Interagency Advisory Council, and the Federal Emergency Management Agency. HSIN will continue to provide operational capabilities for the Command Center and the White House Situation Room, and will remain the single national level hub pertaining to domestic incident management across Emergency Operations Centers at the Federal, State, US Territories, local, private, and public domains to help detect, prevent, and deter terrorists. The Common Operating Picture and Database system will be implemented nationwide for all homeland security partners, for all hazards, and for all threats.

During the next several years, we will focus on developing robust capabilities to assess intelligence collected domestically and abroad and to collect information from a wide variety of sources. That information will be mapped against the Nation's vulnerabilities, allowing the Department to issue timely and actionable preventive and protective measures. We will also implement a comprehensive national indications and warning infrastructure with the capacity to provide timely, effective warnings for specific and imminent threats. In addition, the Department will build secure mechanisms and systems for exchanging sensitive homeland security and critical infrastructure information with homeland security officials, using the best features of existing Federal, state, local and private systems. Further, the Department will build an enhanced identification and tracking capability of the maritime approaches and offshore transit routes of the United States.

## Strategic Goal 2 Prevention

Detect, deter and mitigate threats to our homeland.



### Serving the Public

Recently published air cargo security rules help prevent the use of air cargo as a means of attacking aircraft. The rules mark the first substantial changes to air cargo regulations since 1999, and represent a joint government-industry vision of an enhanced security baseline. These new measures will be enforced by an expanded force of air cargo inspectors, who will be stationed at the 102 airports where 95 percent of domestic air cargo originates.

**T**o fully support this strategic goal, we developed subordinate strategic objectives with supporting performance goals for programs. For each performance goal, we developed quantitative performance measures. Collectively, these measures assess progress in attainment of our strategic goal of Prevention.

The table below correlates our strategic objectives with the performance goals established for each objective, indicated by an objective number in the left hand column. The chart also indicates the estimated net cost of efforts to achieve the objective.



STRATEGIC GOAL 2 - PREVENTION							
STRATEGIC OBJECTIVES SUPPORTING GOAL 2							FY 06 Net Cost (in millions)
2.1 Secure our borders against terrorists, means of terrorism, illegal drugs and violations of trade and immigration laws.							\$ 7,928.6
2.2 Enforce trade and immigration laws.							\$ 3,184.8
2.3 Provide operational end users with the technology and capabilities to detect and prevent terrorist attacks, means of terrorism and other illegal activities.							\$ 2,884.6
2.4 Coordinate national and international policy, law enforcement, and other actions to prevent terrorism.							\$ 925.1
2.5 Strengthen the security of the Nations transportation systems.							\$ 3,489.7
2.6 Ensure the security and integrity of the immigration system.							\$ -3.4
<b>PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES</b>							<b>Detail on Page</b>
2.1		2.4				Improve the targeting, screening, and apprehension of high-risk international cargo and travelers to prevent terrorist attacks, while providing processes to facilitate the flow of safe and legitimate trade and travel. (Border Security Inspections and Trade Facilitation at Ports of Entry)	85
2.1		2.3				To gain operational control of the U.S. border in areas deemed as high priority for terrorist threat potential or other national security objectives. (Border Security and Control between Ports of Entry)	89
		2.3				Improve the threat and enforcement information available to decision makers from legacy and newly developed systems for the enforcement of trade rules and regulations and facilitation of U.S. trade. (Automation Modernization)	90
2.1						Deny the use of air, land and coastal waters for conducting acts of terrorism and other illegal activities against, the United States. (Air and Marine Operations)	92
		2.3				Develop the systems architecture, conduct all associated systems engineering, and develop technology roadmaps for risk areas in nuclear detection. (Domestic Nuclear Detection Systems Engineering and Architecture)	92

NOTE 1: The Net Cost measures the cost of supporting that entire strategic objective, not just the performance goal(s) identified in the table.

NOTE 2: Net cost for Objective 2.6 is negative due to offsetting revenue. See explanations on page 71.

## STRATEGIC GOAL 2 - PREVENTION

### STRATEGIC OBJECTIVES SUPPORTING GOAL 2

2.1 Secure our borders against terrorists, means of terrorism, illegal drugs and violations of trade and immigration laws.

2.2 Enforce trade and immigration laws.

2.3 Provide operational end users with the technology and capabilities to detect and prevent terrorist attacks, means of terrorism and other illegal activities.

2.4 Coordinate national and international policy, law enforcement, and other actions to prevent terrorism.

2.5 Strengthen the security of the Nations transportation systems.

2.6 Ensure the security and integrity of the immigration system.

#### PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES

Detail  
on  
Page

		2.3		Incrementally design, develop, acquire, and support the deployment of a system capable of rapid and high - reliability detection and identification of special nuclear material with out restriction to commerce. (Domestic Nuclear Detection Systems Development and Acquisition)	93
		2.3		Develop the future nuclear detection technologies that will be capable of detecting all nuclear material entering the United States Homeland. (Domestic Nuclear Detection Transformational Research and Development)	94
		2.3		Develop the tools and methodology for and to assess the Nation's domestic nuclear detection capabilities through a combination of developmental and operational test and evaluation, as well as active red - teaming exercises. (Domestic Nuclear Detection Assessments)	95
		2.3		Establish and maintain a real-time situational awareness and support capability for the national nuclear detection architecture, including information analysis, technical reachback, and the development of training and operational response protocols. (Domestic Nuclear Detection Operations Support)	96
		2.4		Accredit all Federal law enforcement training. (Accreditation)	96
		2.4		Provide the knowledge and skills to enable law enforcement agents and officers to fulfill their responsibilities. (Law Enforcement Training)	97
2.2				Remove all removable aliens from the United States. (Detention and Removal)	98

## STRATEGIC GOAL 2 - PREVENTION

### STRATEGIC OBJECTIVES SUPPORTING GOAL 2

2.1 Secure our borders against terrorists, means of terrorism, illegal drugs and violations of trade and immigration laws.

2.2 Enforce trade and immigration laws.

2.3 Provide operational end users with the technology and capabilities to detect and prevent terrorist attacks, means of terrorism and other illegal activities.

2.4 Coordinate national and international policy, law enforcement, and other actions to prevent terrorism.

2.5 Strengthen the security of the Nations transportation systems.

2.6 Ensure the security and integrity of the immigration system.

#### PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES

**Detail  
on  
Page**

	2.2				Prevent the exploitation of systemic vulnerabilities in trade and immigration that allow foreign terrorists, other criminals, and their organizations to endanger the American people, property, and infrastructure. (Office of Investigations)	99
2.1					Enable Federal Immigration and Border Management agencies to make timely and accurate risk and eligibility decisions through coordination of screening capability policies, business strategy and processes, data, information systems, and technology to further enhance security and immigration, travel, and credentialing experiences. (Screening Coordination and Operations Office (SCO) Now US-VISIT)	113
		2.3			Provide dependable risk analyses, effective systems for surveillance and detection, and reliable bioforensic analyses to protect the nation against biological attacks. (Biological Countermeasures)	100
		2.3			Provide dependable risk analyses, effective systems for surveillance, detection, and cleanup, and reliable chemical forensic analyses to protect the nation against chemical attacks. (Chemical Countermeasures)	101
		2.3			Improve explosives countermeasures technologies and procedures to prevent attacks on critical infrastructure, key assets, and the public. (Explosives Countermeasures)	101

## STRATEGIC GOAL 2 - PREVENTION

### STRATEGIC OBJECTIVES SUPPORTING GOAL 2

2.1 Secure our borders against terrorists, means of terrorism, illegal drugs and violations of trade and immigration laws.

2.2 Enforce trade and immigration laws.

2.3 Provide operational end users with the technology and capabilities to detect and prevent terrorist attacks, means of terrorism and other illegal activities.

2.4 Coordinate national and international policy, law enforcement, and other actions to prevent terrorism.

2.5 Strengthen the security of the Nations transportation systems.

2.6 Ensure the security and integrity of the immigration system.

#### PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES

Detail  
on  
Page

2.3

Advance capabilities for threat discovery and awareness, information management and sharing, linkage of threats with vulnerabilities, and capability and motivation assessments for terrorist organizations. (Threat Awareness Portfolio)

102

2.3

Develop effective technologies and tools to increase the capabilities of the Department of Homeland Security operational components to execute their mission to secure the homeland. (Support to Department of Homeland Security Components)

103

2.3

Establish and sustain a coordinated university - based research, development and education system to enhance the Nation's homeland security. (University Programs)

104

2.3

Develop well - designed standards and test and evaluation protocols for products, services, and systems used by the Department of Homeland Security and its partners to ensure consistent and verifiable effectiveness. (Standards)

102

2.3

Prevent terrorist attacks by developing effective capabilities to characterize, assess, and counter new and emerging threats. (Emerging Threats)

105

2.3

Identify and rapidly develop, prototype, and commercialize innovative technologies to thwart terrorist attacks. (Rapid Prototyping)

105



## STRATEGIC GOAL 2 - PREVENTION

### STRATEGIC OBJECTIVES SUPPORTING GOAL 2

2.1 Secure our borders against terrorists, means of terrorism, illegal drugs and violations of trade and immigration laws.

2.2 Enforce trade and immigration laws.

2.3 Provide operational end users with the technology and capabilities to detect and prevent terrorist attacks, means of terrorism and other illegal activities.

2.4 Coordinate national and international policy, law enforcement, and other actions to prevent terrorism.

2.5 Strengthen the security of the Nations transportation systems.

2.6 Ensure the security and integrity of the immigration system.

#### PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES

**Detail  
on  
Page**

		2.3			Provide effective and economical capabilities to dramatically reduce the threat to commercial aircraft posed by man-portable anti-aircraft missiles. [Counter Man-Portable Air Defense System (MANPADS)]	106
		2.3			Ensure interoperability and compatibility between emergency response agencies at the local, state, and federal levels and standardize federal testing and evaluation efforts for emergency response technologies. (Interoperability & Compatibility)	107
		2.3			Produce actionable information and recommend reliable technologies to help protect U.S. critical infrastructure. (Critical Infrastructure Protection)	107
		2.3			Enable the creation of and migration to a more secure critical information infrastructure. (Cyber Security)	108
		2.3			Encourage the development and deployment of anti-terrorism technologies by awarding SAFETY Act benefits to homeland security technology producers. (SAFETY Act)	109
		2.3		2.5	Reduce the probability of a successful terrorist or other criminal attack to the air transportation system by improved passenger and baggage screening processes. (Aviation Security)	109
				2.5	Reduce the probability of a successful terrorist or other criminal attack on surface transportation systems through the issuing of standards, compliance inspections, and vulnerability assessments. (Surface Transportation Security)	111

## STRATEGIC GOAL 2 - PREVENTION

### STRATEGIC OBJECTIVES SUPPORTING GOAL 2

2.1 Secure our borders against terrorists, means of terrorism, illegal drugs and violations of trade and immigration laws.

2.2 Enforce trade and immigration laws.

2.3 Provide operational end users with the technology and capabilities to detect and prevent terrorist attacks, means of terrorism and other illegal activities.

2.4 Coordinate national and international policy, law enforcement, and other actions to prevent terrorism.

2.5 Strengthen the security of the Nations transportation systems.

2.6 Ensure the security and integrity of the immigration system.

#### PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES

Detail  
on  
Page

2.5

Promote confidence in our nation's civil aviation system through the effective deployment of Federal Air Marshals to detect, deter, and defeat hostile acts targeting U.S. air carriers, airports, passengers, and crews. (Federal Air Marshall Service)

112

2.5

Eliminate maritime fatalities and injuries on our Nations oceans and waterways. (Marine Safety)

114

2.1

Reduce the flow of illegal drugs entering the U.S. via non - commercial maritime shipping sources. (Drug Interdiction)

115

2.1

Eliminate the flow of undocumented migrants via maritime routes to the U.S. (Migrant Interdiction)

116

2.1

Reduce the numbers of vessel incursions into the United States Exclusive Economic Zone (EEZ). (Other law enforcement)

117

2.4

Support our national security and military strategies by ensuring assets are at the level of readiness required by the combatant commander. (Defense Readiness)

118

2.6

Enhance the integrity of the legal immigration system. (Immigration Security and Integrity)

119

## HIGHLIGHTS

**S**ome of the key performance measures used to gauge success in achieving the goal of *Prevention* are highlighted below. These measures illustrate some of our significant accomplishments during FY 2006 in achieving *Prevention* goals and objectives.

The Department of Homeland Security uses a risk-based approach to identify preventive and protective steps that increase security, and in turn, reduces the risk of harm to the Homeland. A quantifiable overall measurement of risk reduction would be an ideal measure; however, there is not a straightforward way of calculating total risk reduction to all aspects of our Homeland at this time. Yet, the measures below show the Department's progress in addressing risk reduction by improving *Prevention*.

- **US-VISIT's biometric program keeps terrorists and other criminals out of our country.**

Measure: *Number of biometric watch list hits for visa applicants processed at consular offices.* (Target Met) (See Page 113)

US-VISIT's biometric program increased watch list hits by 185% at consular offices. Keeping terrorists and other criminals out of our country helps protect the American people, while facilitating visits from those who are legitimate and appropriate. In FY 2006 there were 2558 watch list hits at consular offices, up from 897 hits in FY 2005. US-VISIT is part of a continuum of biometrically-enhanced security measures that begins outside U.S. borders and continues through a visitor's arrival in and departure from the United States. When the visitor arrives in the United States, US-VISIT procedures allow the Department of Homeland Security to determine whether the person applying for entry is the same person who was issued the visa by the Department of State, and additional watch list checks improve the Department's ability to make admissibility decisions. Biometrics has allowed the Department, through US VISIT, to deny entry to more than 1,100 known criminals and visa violators. US VISIT has stopped murderers, pedophiles, drug traffickers and immigration violators from entering the United States through biometrics and international cooperation.

- **The Department has increased the number of containers inspected prior to entering the United States.**

Measure: *Percent of worldwide U.S. destined containers processed through Container Security Initiative.* (Target Met) (See Page 87)

One of the primary outcomes of the Container Security Initiative (CSI) program is that of deterrence-to prevent containers with Weapons of Mass Destruction or Effect (WMD/E) from arriving at U.S. ports. This measure shows the percent of U.S. destined cargo processed through Container Security Initiative ports prior to the cargo being loaded, divided by the annual worldwide number of containers destined for the U.S. In FY 2006, CSI ports processed 81.7% of all containers destined for the United States prior to loading, up from 73.4% in FY 2005. CSI officials work in tandem with foreign customs administrations using advanced technology, trade data and expanded collaboration to identify cargo containers that pose a potential risk for terrorism. Those containers are inspected at the foreign ports before being loaded on to vessels destined to the United States. The actual result achieved by the CSI program - having a higher percentage of U.S. destined cargo targeted, screened, reviewed, and processed through CSI ports - increases the likelihood of apprehending high-risk international cargo and travelers to prevent terrorist attacks, while facilitating the flow of safe and legitimate trade and travel from more foreign ports. The goal by 2010 is for CSI ports to process 86 percent of all containers destined for the United States prior to loading.

- **We are removing more illegal aliens.**

Measure: *Number of aliens removed each quarter as a fraction of those ordered to be removed each quarter.* (Target Met) (See Page 98)

The increased number of fugitive operations teams in FY 2006 has paid off with a healthy 124.37% removal rate, up significantly from our FY 2005 performance of 109%. With certain exceptions, an alien illegally in the United States is "removable" when an immigration judge issues a "final order of removal" or administrative orders are issued per statute. This measure indicates the number of aliens removed during a quarter as a fraction of those ordered "removed" during the same quar-

ter—not necessarily the same aliens. This means we have started to remove aliens who were not removed in the past that should have been removed.

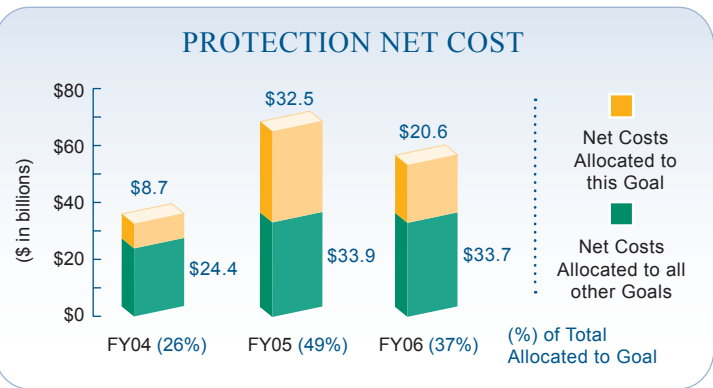
In addition, we measure the percentage of system-wide airport compliance with security regulations. During FY 2006, 96.8% of our nation's airports were compliant with security regulations. This is up slightly from FY 2005 performance of 96.3%. Through regulatory compliance activities, the Department seeks to reduce the probability of a successful terrorist attack or other criminal attack to the air transportation system. The Transportation Security Administration's compliance and enforcement program protects the Nation's transportation system by conducting inspections, investigations and assessments that ensure compliance with aviation transportation security laws, regulations, directives and agreements. By inspecting and gauging industry's compliance with those rules, the Transportation Security Administration can identify security gaps and vulnerabilities and then work to close any deficiencies. In the near term, sustained high rates of compliance with these rules leads to practical improvements in security and reduces the overall risk to the transportation sector. In the long term, we are working to refine this performance measure to provide quantitative measurement of the risk to the public that has been reduced as a result of implementing these program objectives.

## FUTURE STEPS

**T**he Department's main priority is to prevent further terrorist attacks against the nation. By managing who and what enters the United States, we will work to prevent the entry of terrorists and instruments of terror while facilitating the legitimate flow of people, goods and services. During the next five years, the Department will continue to create coherent screening, targeting and risk-management approaches across activities, including the capacity for transmitting and receiving advanced information about people and commercial shipments approaching the United States. We will enhance real-time monitoring and surveillance of the border, including seaports, landports, airports, and between ports of entry. The Department will build an integrated system that detects, identifies and tracks high-threat vehicles in the air, land and maritime domains, and share this information with those that can take action against the threat. We will implement a program to identify, track and intercept chemical, biological, radiological, nuclear and explosive components and systems at ports of entry and, where practicable, in intermodal transportation systems within U.S. borders. Additionally, the Department will continue to increase apprehension rates and ensure that detention space is available to support our detention and removal efforts.

## Strategic Goal 3 Protection

Safeguard our people and their freedoms, critical infrastructure, property and the economy of our nation from acts of terrorism, natural disasters or other emergencies.



### Serving the Public

Working closely with state and local officials, other Federal agencies, and the private sector, the Department helps to ensure that proper steps are taken to protect critical infrastructure, property and the economy of our nation from acts of terrorism, natural disasters or other emergencies. America's critical infrastructure, includes food and water systems, agriculture, health systems and emergency services, information and telecommunications, banking and finance, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, ports, waterways), the chemical and defense industries, postal and shipping entities, and national monuments and icons.

**T**o fully support this strategic goal, we developed subordinate strategic objectives with supporting performance goals for programs. For each performance goal, we developed quantitative performance measures. Collectively, these measures assess progress in attainment of our strategic goal of Protection.

The table below correlates our strategic objectives with the performance goals established for each objective, indicated by an objective number in the left hand column. The chart also indicates the estimated net cost of efforts to achieve the objective.

STRATEGIC GOAL 3 - PROTECTION							
STRATEGIC OBJECTIVES SUPPORTING GOAL 3							FY 06 Net Cost (in millions)
3.1 Protect the public from acts of terrorism and other illegal activities.							\$ 1,870.3
3.2 Reduce infrastructure vulnerability from acts of terrorism.							\$ 930.0
3.3 Protect our Nations financial infrastructure against crimes, to include currency and financial payment systems.							\$ 402.0
3.4 Secure the physical safety of the President, Vice President, visiting world leaders and other protectees							\$ 1,051.0
3.5 Ensure the continuity of government operations and essential functions in the event of crisis or disaster.							\$ 70.3
3.6 Protect the marine environment and living marine resources.							\$ 971.1
3.7 Strengthen nationwide preparedness and mitigation against acts of terrorism, natural disasters, or other emergencies.							\$ 16,288.1
PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES							Detail on Page
					3.7	Reduce the impact of natural hazards on people and property through the analysis and reduction of risks and the provision of flood insurance. (Mitigation)	120
					3.7	Help ensure the nation is ready to respond to and recover from acts of terrorism, natural disasters, or other emergencies through implementation of the National Incident Management System (NIMS) and the provision of emergency management training. (Readiness)	122
				3.5		Ensure all Federal Departments and Agencies have fully operational Continuity of Operations (COOP) and Continuity of Government (COG) capabilities. (National Security)	123
3.1	3.2			3.5		Complete and continuous law enforcement and security protection of federally controlled facilities, their tenants, and the visiting public. (Protection of Federal Assets - Federal Protective Service)	124
	3.2				3.7	Strengthen the Nation's capacity to prepare for and respond to natural or other disasters. (National Preparedness Leadership and Coordination)	125

NOTE: The Net Cost measures the cost of supporting that entire strategic objective, not just the performance goal(s) identified in the table.



## STRATEGIC GOAL 3 - PROTECTION

## STRATEGIC OBJECTIVES SUPPORTING GOAL 3

### 3.1 Protect the public from acts of terrorism and other illegal activities.

### 3.2 Reduce infrastructure vulnerability from acts of terrorism.

3.3 *Protect our Nations financial infrastructure against crimes, to include currency and financial payment systems.*

### 3.4 Secure the physical safety of the President, Vice President, visiting world leaders and other protectees

*3.5 Ensure the continuity of government operations and essential functions in the event of crisis or disaster.*

### 3.6 Protect the marine environment and living marine resources.

*3.7 Strengthen nationwide preparedness and mitigation against acts of terrorism, natural disasters, or other emergencies.*

## PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES

**Detail  
on  
Page**

	3.2					3.7	Protect the Nations high risk and most valued critical infrastructure and key resources (CI/KR) by characterizing and prioritizing assets, modeling and planning protective actions, building partnerships, and issuing targeted infrastructure protection grants. (Infrastructure Protection)	125
	3.2						Improve the security of America's cyber and emergency preparedness telecommunications assets by working collaboratively with public, private, and international entities. (Cyber Security & Telecommunications)	127
						3.7	Enhance the Nations preparedness by increasing the capability of states, territories, and local jurisdictions to prevent, protect against, respond to, and recover from terrorism and all - hazard events through the provision of grants, first responder training, technical assistance, and exercises. (Grants, Training & Exercise)	128
						3.7	Ensure a coordinated and unified approach to represent medical readiness among the United States health community by providing data - driven, scientifically based policy and advice to advocate public health needs. (Medical Coordination)	131

## STRATEGIC GOAL 3 - PROTECTION

### STRATEGIC OBJECTIVES SUPPORTING GOAL 3

3.1 Protect the public from acts of terrorism and other illegal activities.

3.2 Reduce infrastructure vulnerability from acts of terrorism.

3.3 Protect our Nations financial infrastructure against crimes, to include currency and financial payment systems.

3.4 Secure the physical safety of the President, Vice President, visiting world leaders and other protectees

3.5 Ensure the continuity of government operations and essential functions in the event of crisis or disaster.

3.6 Protect the marine environment and living marine resources.

3.7 Strengthen nationwide preparedness and mitigation against acts of terrorism, natural disasters, or other emergencies.

#### PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES

Detail  
on  
Page

3.7  
Maximize the health and safety of the public and firefighting personnel against fire and fire - related hazards by providing assistance to fire departments and by training the Nations fire responders and health care personnel to prevent, protect against, respond to, and recover from fire - related events. (Fire Prevention Assistance)

132

3.6  
Achieve sustained fisheries regulation compliance on our Nations Oceans. [Living Marine Resources (LMR)]

133

3.1  
Reduce homeland security risk in the maritime domain. [Ports Waterways and Coastal Security (PWCS)]

134

3.4  
Protect our nation's leaders and other protectees. [Domestic Protectees (DP)]

135

3.4  
Protect visiting world leaders. [Foreign Protectees and Foreign Missions (FP/ FM)]

135

3.4  
Reduce threats posed by global terrorists and other adversaries. [Protective Intelligence (PI)]

136

## STRATEGIC GOAL 3 - PROTECTION

## STRATEGIC OBJECTIVES SUPPORTING GOAL 3

### 3.1 Protect the public from acts of terrorism and other illegal activities.

### 3.2 Reduce infrastructure vulnerability from acts of terrorism.

*3.3 Protect our Nations financial infrastructure against crimes, to include currency and financial payment systems.*

### 3.4 Secure the physical safety of the President, Vice President, visiting world leaders and other protectees

*3.5 Ensure the continuity of government operations and essential functions in the event of crisis or disaster.*

### 3.6 Protect the marine environment and living marine resources.

*3.7 Strengthen nationwide preparedness and mitigation against acts of terrorism, natural disasters, or other emergencies.*

## PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES

**Detail  
on  
Page**

Reduce losses to the public attributable to counterfeit currency, other financial crimes, and identity theft crimes that are under the jurisdiction of the Secret Service, which threaten the integrity of our currency and the reliability of financial payment systems worldwide. [Financial Investigations (FI)]

136

Reduce losses to the public attributable to electronic crimes and crimes under the jurisdiction of the Secret Service that threaten the integrity and reliability of the critical infrastructure of the country. (Infrastructure Investigations)

137

## HIGHLIGHTS

**S**ome of the key performance measures used to gauge success in achieving the goal of Protection are highlighted below. These measures illustrate some of our significant accomplishments during FY 2006 in achieving Protection goals and objectives.

The Department of Homeland Security uses a risk-based approach to identify preventive and protective steps that increase security, and in turn, reduces the risk of harm to the Homeland. A quantifiable overall measurement of risk reduction would be an ideal measure; however, there is not a straightforward way of calculating total risk reduction to all aspects of our Homeland at this time. Yet, the measures below show the Department's progress in addressing risk reduction by improving Protection.

- **Buffer Zone Protection plans help protect communities from potential terrorist attacks against chemical facilities.**

Measure: *Percent of high-priority critical infrastructure for which a Buffer Zone Protection Plan (BZPP) has been implemented.* (Target Met) (See Page 126)

The Department achieved 58% in FY 2006, up significantly from our FY 2005 percentage of 18%. This measure calculates the percent of critical infrastructure that has an implemented Buffer Zone Protection (BZP) Plan. Buffer Zone Protection planning contributes to reducing specific vulnerabilities by developing protective measures that extend from the critical infrastructure site to the surrounding community to deny terrorists an operational environment. The Department works in collaboration with state, local, and tribal entities by providing training workshops, seminars, technical assistance and a common template to standardize the BZP development process.

- **The Secret Service continued its 100% protection rate of our nation's leaders.**

Measure: *Percentage of Instances Protectees Arrive and Depart Safely.* (Target Met) (See Page 135)

One hundred percent protection is the only acceptable goal, and this was achieved during FY 2006. To safeguard our nation's leaders, the Department operates the Domestic Protectees program 24 hours a day, 365 days a year to protect the President and Vice President and their families, former Presidents and their spouses, and other individuals designated by statute or Presidential directive. As a rule, the threat posed and the level of effort required to provide security increases dramatically when a protectee is traveling. Therefore, the Department measures the percentage of travel stops where the protectee arrives and departs safely.

- **Federal, state, local and tribal governments are better able to protect against acts of terrorism, natural disasters, or other emergencies.**

Measure: *Percent of Federal, State, Local and Tribal Governments compliant with the National Incident Management System (NIMS).* (Target Met) (See Page 122)

The percent of Federal, state, local and tribal governments that are compliant with NIMS, for FY 2006 was 100%, up from 82%. Agencies compliant with NIMS are better able to protect against acts of terrorism, natural disasters, or other emergencies. To strengthen nationwide preparedness and mitigation against acts of terrorism, natural disasters, or other emergencies, the Department has implemented the Nation's first standardized management approach that unifies Federal, state, and local lines of government for incident response. The National Incident Management System (NIMS) establishes standardized processes, protocols, and procedures that all responders - Federal, state, tribal, and local - will use to coordinate and conduct response actions. With responders using the same standardized procedures, they will all share a common focus in national preparedness and readiness in responding to and recovering from an incident should one occur.

- **Seventeen sector-specific plans that complement the NIPP and detail the risk management framework will be released in December 2006.**

Through the National Infrastructure Protection Plan (NIPP), the Department has established a comprehensive risk manage-

ment framework that clearly defines the roles and responsibilities among government, private industry, nongovernmental agencies and other key partners in protecting our nation's critical infrastructure, enhancing additional security measures and focusing resources according to risk. Developed in collaboration with sector specific security partners, these plans will address unique characteristics and risk landscapes that include such areas as agriculture and food; energy; public health and healthcare; banking and finance; drinking waters and water treatment systems; information technology; telecommunications; postal and shipping; transportation systems including mass transit, aviation, maritime, ground or surface, and rail and pipeline systems; chemical; commercial facilities; government facilities; emergency services; dams; nuclear reactors, materials and waste; the defense industrial base; and national monuments and icons.

## FUTURE STEPS

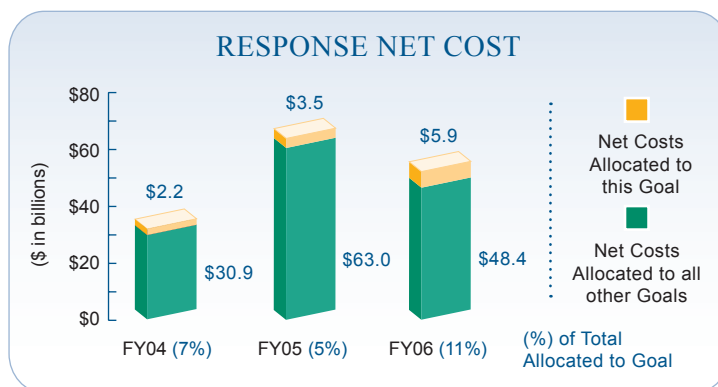
**T**he Department is leading a systemic, comprehensive and strategic effort to reduce the country's vulnerability to terrorist attack and other illegal activities, to protect the public, to protect critical infrastructure, to protect our Nation's financial infrastructure, to protect key heads of state (President and Vice President), to protect the marine environment and to protect government operations and essential functions in the event of crisis or disaster.

During the next five years, the Department will continue strengthening the National Incident Management System (NIMS) to develop incident management expertise, interoperable standards for incident response, and maintain and provide a forum for increased dialog and cross training among response communities. We will also develop a single, comprehensive and seamless incident command apparatus using the capabilities, assets and expenditures of all departmental entities. We are strengthening Federal law enforcement communities, augmenting the scope and quality of information available to them, and providing tools to assist them in stopping those who wish to do this country harm. We will continue to integrate law enforcement functions to maximize effectiveness and minimize duplication. We will create a rigorous document fraud detection and development system that produces documents of high integrity, while thwarting forgeries and fabrications.

The Department's work in improving our ability to detect and prevent chemical, biological, radiological and nuclear threats to the nation will reduce our vulnerability. We are establishing national priorities in the development of technologies to recognize, identify and confirm the occurrence of a terrorist attack and thereby minimize casualties. The Department will strengthen the nation's preparedness by focusing Federal, state and local efforts on a cohesive, mutually reinforcing response capability.

## Strategic Goal 4 Response

Lead, manage and coordinate the national response to acts of terrorism, natural disasters or other emergencies.



### Saving the Public

Survival Technician 2nd Class Dennis Moyer of Coast Air Station San Francisco is presented an Air Medal by Rear Jody Breckenridge, Commander of the 11th Coast Guard. Moyer rescued a woman in her near-fully submerged car waters on New Year's Eve near Ukiah, California. He and the team from Air Station San Francisco were assisting local emergency agencies in northern California during torrential rains. They spotted the woman. After being lowered from the helicopter, Moyer had to fight swiftly moving waters to cut the woman's seat belt while also holding her head above water. The medal is awarded to military personnel for heroic meritorious achievement while participating in aerial flight.

To fully support this strategic goal, we developed subordinate strategic objectives with supporting performance goals for programs. For each performance goal, we developed quantitative performance measures. Collectively, these measures assess progress in attainment of our strategic goal of Response.

The table below correlates our strategic objectives with the performance goals established for each objective, indicated by an objective number in the left hand column. The chart also indicates the estimated net cost of efforts to achieve the objective.



STRATEGIC GOAL 4 - RESPONSE				
STRATEGIC OBJECTIVES SUPPORTING GOAL 4				FY 06 Net Cost (in millions)
4.1 Reduce the loss of life and property by strengthening response readiness.				\$ 428.0
4.2 Provide scalable and robust all-hazard response capability.				\$ 5,119.4
4.3 Provide search and rescue services to people and property in distress.				\$ 993.8
<b>PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES</b>				<b>Detail on Page</b>
4.1	4.2		Ensure the capability and readiness of all FEMA disaster response teams and logistics capabilities to respond quickly and effectively to provide assistance when and where needed. (Response)	138
		4.3	Save mariners in imminent danger on our Nations oceans and waterways. [Search and Rescue (SAR)]	140
4.1	4.2		Eliminate oil spills and chemical discharge incidents. [Marine Environmental Protection (MEP)]	140

NOTE: The Net Cost measures the cost of supporting that entire strategic objective, not just the performance goal(s) identified in the table.

## HIGHLIGHTS

Some of the key performance measures used to gauge success in achieving the goal of Response are highlighted below. These measures illustrate some of our significant accomplishments during FY 2006 in achieving Response goals and objectives.

The Department of Homeland Security uses a risk-based approach to identify preventive and protective steps that increase security, and in turn, reduces the risk of harm to the Homeland. A quantifiable overall measurement of risk reduction would be an ideal measure; however, there is not a straightforward way of calculating total risk reduction to all aspects of our Homeland at this time. Yet, the measures below show the Department's progress in addressing risk reduction by improving Response.

- **FEMA's average response time to arrive at a disaster scene has improved.**

Measure: *Average response time in hours for emergency response teams to arrive on scene.* (Target Met) (See page 139)

Arriving at an emergency quickly shows the Department's ability to respond to disasters. With a goal of 48 hours for Federal response teams to arrive on scene at a disaster site, during FY 2006 our average response time was 25 hours. The Department provides Federal response to catastrophic events and natural disasters when state and local governments lack the ability to respond adequately. Improving the timeliness of specialized Federal response teams has saved lives, reduced property loss, enabled greater continuity of services, and enhanced logistical capability in the

wake of disasters.

This reduction in time for emergency response teams to be operational on the scene will greatly improve the impact to lives saved, loss of property, available services, and logistics capability.

- **The Coast Guard continues to rescue mariners in imminent danger.**

Measure: *Percent of mariners in imminent danger saved.* (Target Not Met) (See page 140)

Minimizing the loss of life, injury, and property damage by rendering aid to persons in distress is a Department priority. We seek to prevent loss of life in every situation where our efforts could possibly be brought to bear. In FY 2006, the U.S. Coast Guard rescued 85.3% of mariners in imminent danger. This is slightly down from our FY 2005 results of 86.1%. The number of recreational and commercial maritime users continues to increase as more Americans move to coastal areas and as global trade continues to grow. Every day the U.S. Coast Guard Search and Rescue program saves mariners in imminent danger on our Nation's waterways and oceans. To further increase the number of lives saved, the Department is investing in new response capabilities, including the Response Boat Medium and wider implementation of the Rescue-21 communications system. Moreover, we are improving prevention activities, including safe boater programs to reduce the overall risk to mariners. These investments combine to increase the probability that a search and rescue mission will end with lives saved instead of lost.

## FUTURE STEPS

Improving the nation's ability to respond to disasters, man-made or natural, is a top priority for the Department. Incorporating lessons learned from Hurricane Katrina and other disasters, the Department is improving its capabilities and preparing those who respond to acts of terror and other emergencies. Our priority is ensuring connectivity and interoperability with the appropriate Federal, state and local entities that are accountable for response.

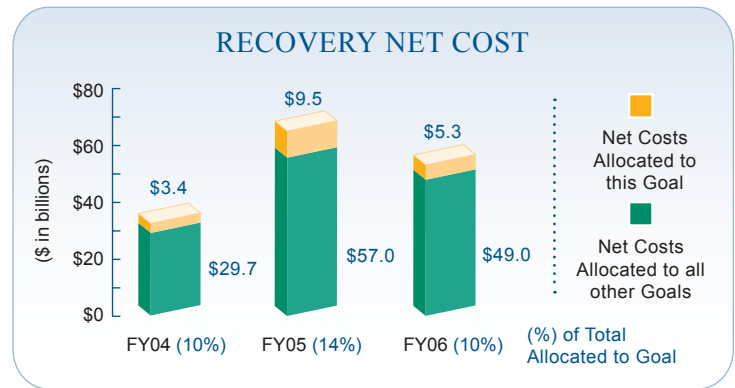
The Department will implement an interoperable, safe and reliable communications system to ensure an effective response to crisis. Additionally, we will build a comprehensive package of strategically pre-positioned response equipment, available trained personnel, supplies and transportation assets.

We will strengthen the nation's ability to respond to emergencies by integrating departmental response systems and teams and completing catastrophic all-hazard plans for the most vulnerable communities. The Department will provide health and medical response readiness through integrated planning, surge capacity capabilities and availability of vaccines and medical supplies to address health and medical emergencies or acts of terrorism. We will deliver emergency housing to large displaced populations following major disasters. We will provide a Federal medical response capability that supplements state and local disaster response by: enhancing National Disaster Medical System team readiness and capability, reducing the average team response time, and increasing the percentage of fully operational Disaster Medical Assistance teams. The Department will coordinate an effective response when state, local and tribal resources are overwhelmed.

To assist mariners in distress, the U.S. Coast Guard will replace 41-foot utility boats and other large non-standard boats with assets more capable of meeting all of their multi-mission operational requirements. The response boat-medium will greatly improve the Coast Guard's small boat Search and Rescue response capability by providing increased speed, enhanced ability to handle greater sea conditions, and improved electronics, thereby providing the opportunity to save more lives.

## Strategic Goal 5 Recovery

Lead national, state, local and private-sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters or other emergencies.



### Serving the Public

Army Corps of Engineer Herbie Petit and Plaquemines Parish Flood Gate Operator John Machella point to some pumps in Empire, Orleans, LA, used to pump water out from between a temporary ber dam and the Flood Gate so repairs can be made. FEMA is helping Parrish government repair the Flood Gate that was damaged by hurricane Katrina under its Public Assistance Program.

**T**o fully support this strategic goal, we developed subordinate strategic objectives with supporting performance goals for programs. For each performance goal, we developed quantitative performance measures. Collectively, these measures assess progress in attainment of our strategic goal of Recovery.

The table below correlates our strategic objectives with the performance goals established for each objective, indicated by an objective number in the left hand column. The chart also indicates the estimated net cost of efforts to achieve the objective.

STRATEGIC GOAL 5 - RECOVERY			
STRATEGIC OBJECTIVES SUPPORTING GOAL 5			FY 06 Net Cost (in millions)
5.1 Strengthen nationwide recovery plans and capabilities.			\$ 240.8
5.2 Provide scalable and robust all-hazard recovery assistance.			\$ 4,339.3
PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES			Detail on Page
5.1	5.2	Help individuals and communities affected by federally declared disasters return to normal function quickly and efficiently, while planning for catastrophic disaster recovery operations. (Recovery)	142

NOTE: The Net Cost measures the cost of supporting that entire strategic objective, not just the performance goal(s) identified in the table.

## HIGHLIGHTS

Some of the key performance measures used to gauge success in achieving the goal of Recovery are highlighted below. These measures illustrate some of our significant accomplishments during FY 2006 in achieving Recovery goals and objectives.

- **Customer satisfaction with FEMA's recovery assistance has improved.**

Measures: *Percent of customers satisfied with Public Recovery Assistance* (Target Met) (See page 142)

To ensure that individuals and families that have been affected by disasters have access to the full range of response and recovery programs in a timely manner and that the best possible level of service is provided to applicants, the Department seeks to increase the annual customer satisfaction level among recipients, while reducing the program delivery cost and increasing the timeliness of service delivery. With a goal of 90% satisfaction with Individual Recovery Assistance programs, during FY 2006 we achieved a customer satisfaction rating of 91% in response to the question "Overall, how would you rate the information and support you received from FEMA since the disaster occurred?" As much as we try to prepare for catastrophic disasters and to reduce our risk from their devastation, hurricanes, tornadoes, major earthquakes and other disasters still happen. When they do, local and state officials are the first to respond. If the loss of life and property overwhelms this response, the Department's Federal Emergency Management Agency (FEMA) is called upon to help. We measure the important factors of overall customer satisfaction with both Individual Recovery Assistance programs that provide aid to individuals, families and business owners; and with Public Assistance Programs that provide aid to public and certain private non-profit entities for emergency services and for the repair or replacement of disaster-damaged public facilities.

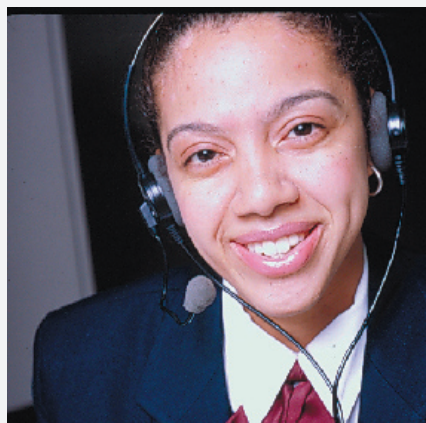
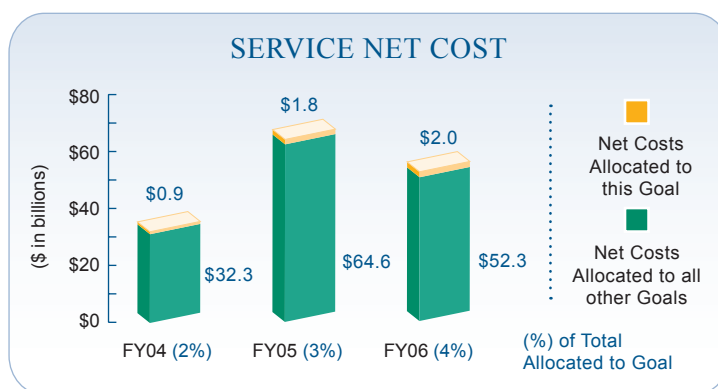
## FUTURE STEPS

The Department leads the nation in coordinating recovery from disasters. In the event of a national emergency, the Department is prepared to lead Federal, state, local and private-sector efforts to help rebuild communities and restore services. We will lead long-term recovery including assessing losses, identifying infrastructure recovery actions and rebuilding the capabilities of local partners. As a result of lessons learned from Hurricane Katrina, the Department is dramatically increasing

the nation's stockpiles of relief supplies, retooling the Federal Emergency Management Agency (FEMA) for the 21st century, updating disaster plans, supporting our state and local partners, and emphasizing individual and community preparedness. The Department is undertaking several new measures designed to strengthen FEMA's essential functions so it can more effectively respond to manmade or natural disasters, particularly during catastrophic events. These new measures are designed to match the experience and skills of FEMA employees with state of the art tools and technology - maximizing the agency's performance regardless of disaster size or complexity. The Department is specifically working to improve FEMA's logistics capabilities, enhance customer service and intake procedures, improve the debris removal process, and build more effective communications capabilities to ensure timely and accurate awareness about conditions and events that unfold during a disaster. As a result, four times the number of emergency meals and ice, and 2.5 times the water are available this year than were available prior to Hurricane Katrina. These supplies have the capacity to sustain 1 million people for a period of one week. Katrina left over 100 million cubic yards of debris in its wake over a span of 90,000 square miles. In order to streamline the debris removal process and ensure quick reimbursement for services, FEMA is establishing solid contracting practices to help communities quickly begin recovery operations. When it makes economic sense, local construction companies will be allowed to more fully participate in debris removal.

## Strategic Goal 6 Service

Serve the public effectively by facilitating lawful trade, travel and immigration.



### Serving the Public

Improving cycle time and customer satisfaction conveys the Department's focus on serving the public. The Department secures America's promise as a nation of immigrants and upholds our time-honored tradition of welcoming those individuals seeking freedom, liberty and an opportunity for a better life. The Department's U.S. Citizenship and Immigration Services (USCIS) seeks to decrease the amount of time it takes to obtain benefits by those who qualify for them, while identifying and denying benefits to those who are ineligible.

**On average, on an annual basis, USCIS:**

- Processes more than 6 million applications;
- Serves more than 20 million customers via the National Customer Service Call Centers;
- Serves approximately 3 million customers through information counters at local offices;
- Processes nearly 90,000 asylum cases;
- Performs more than 90,000 refugee interviews; and
- Conducts the naturalization of approximately half a million new citizens

**T**o fully support this strategic goal, we developed subordinate strategic objectives with supporting performance goals for programs. For each performance goal, we developed quantitative performance measures. Collectively, these measures assess progress in attainment of our strategic goal of Service.

The table below correlates our strategic objectives with the performance goals established for each objective, indicated by an objective number in the left hand column. The chart also indicates the estimated net cost of efforts to achieve the objective.



STRATEGIC GOAL 6 - SERVICE				
STRATEGIC OBJECTIVES SUPPORTING GOAL 6				FY 06 Net Cost (in millions)
6.1 Increase understanding of naturalization, and its privileges and responsibilities.				\$ 0
6.2 Provide efficient and responsive immigration services that respect the dignity and value of individuals.				\$ -108.0
6.3 Support the United States humanitarian commitment with flexible and sound immigration and refugee programs.				\$ 5.1
6.4 Facilitate the efficient movement of legitimate cargo and people.				\$ 1,405.1
<b>PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES</b>				<b>Detail on Page</b>
		6.4	Eliminate collisions, allisions and groundings by vessels on our Nations oceans and waterways. (Aids to Navigation)	144
		6.4	Maintain operational channels for navigation, limiting channel closures to two days (during average winters) and eight days (during severe winters). (Ice Operations)	145
	6.2	6.3	Provide immigration benefit services in a timely, consistent, and accurate manner. (Adjudication Services)	146
	6.2		Provide timely, consistent, and accurate information to our customers. (Information and Customer Service)	148
6.1			Enhance educational resources and promote opportunities to support immigrants' integration and participation in American civic culture. (Citizenship)	149

NOTE 1: The Net Cost measures the cost of supporting that entire strategic objective, not just the performance goal(s) identified in the table.

NOTE 2: Net cost for objectives 6.1, 6.2 and 6.3 are low or negative due to offsetting revenue. See explanations on page 71.

## HIGHLIGHTS

Some of the key performance measures used to gauge success in achieving the goal of Service are highlighted below. These measures illustrate some of our significant accomplishments during FY 2006 in achieving Service goals and objectives.

- **Immigration services has improved.**

Measures: *Actual cycle time to process form I-485 (Application to Register for Permanent Residence or to Adjust Status)* (Target Met), *Actual cycle time to process form I-129 (Petition for Nonimmigrant Worker)* (Target Met), *Actual cycle time to process form N-400 (Application for Naturalization)* (Target Met), and *Customer satisfaction rate with USCIS phone centers* (Target Met) (See pages 146-148)

Improving cycle time and customer satisfaction conveys the Department's focus on serving the public. The Department secures America's promise as a nation of immigrants and upholds our time-honored tradition of welcoming those individuals seeking freedom, liberty and an opportunity for a better life. The Department's U.S. Citizenship and Immigration Services (USCIS) seeks to decrease the amount of time it takes to obtain benefits by those who qualify for them, while identifying and denying benefits to those who are ineligible. The USCIS conducts approximately 135,000 background checks on applicants seeking immigration benefits each day to ensure that appropriate individuals receive them. We provide phone-based assistance to the public to obtain benefits and services offered by the Department, and measure customer satisfaction with service received over the phone. During FY 2006, we experienced an 83% customer satisfaction rating for phone services. We measure cycle time, or the amount of time it takes to provide a decision on an application once it is received, as one way of evaluating the efficiency of our processes. For eligible aliens who seek to become legal permanent residents, "green card" holders, or otherwise adjust status through the I-485 application, the cycle time was 5.9 months meeting our target of less than 6 months and significantly improved from our FY 2005 results of 13.9 months. For those who seek naturalization through the N-400 application, the cycle time was 5.6 months meeting our target of 6 months and also down from our FY 2005 results of 10.9 months. For foreign workers who perform temporary services, provide labor, or receive training through the I-129 petition, the cycle time was 2 months meeting our target, but up from our FY 2005 results of 1.5 months.

In addition, to reopen navigable channels and operational waterways in the aftermath of Hurricane Katrina, the U.S. Coast Guard removed hazards, repaired navigation aids, and facilitated the reconstruction of bridges in the Gulf Region. A few of the results achieved by their efforts are:

More than 2,000 vessels were damaged by Hurricane Katrina and more than 800 vessels caused a potential hazard to navigation. As of August 1, 2006, the Coast Guard has overseen salvage of over 800 of these vessels. Removal of other marine debris (garbage, houses, automobiles, etc.) is ongoing. As a result, no critical navigable waterways are currently obstructed by vessels or marine debris.

1,789 aids to navigation (day markers, buoys, etc.), including 73 ranges, were damaged or destroyed by Hurricane Katrina. Currently, all ports are open without restrictions and all aids to navigation have been repaired with permanent or temporary markers.

The Coast Guard Bridge Program has facilitated reconstruction of over 70 damaged or destroyed bridges impacting navigable waterways in the Gulf Coast region. As of August 1, 2006, approximately 95% of the damaged bridges have been placed back in service, and the Coast Guard is working closely with local and state governments to expedite construction on those bridges still requiring repairs or replacement.

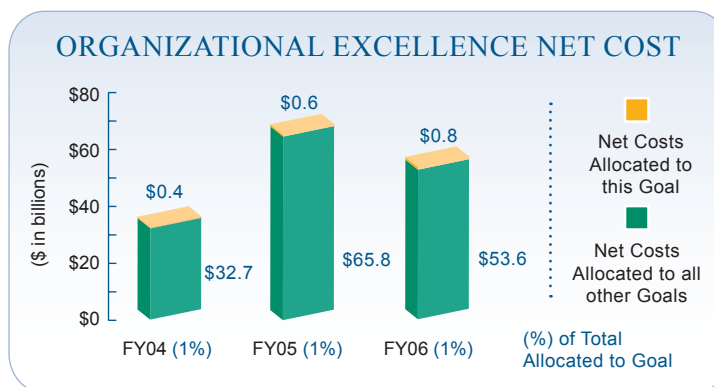
## FUTURE STEPS

**T**he United States will continue to welcome legitimate visitors and those seeking opportunities within our nation, while preventing terrorists and their supporters from entering the country. During the next five years, the Department will eliminate burdensome management and support functions and modernize immigration services by restructuring our business processes, implementing electronic filing and conducting virtual adjudications. These changes will continue to build upon the progress achieved at the end of FY 2006 in significantly reducing the immigration application backlog resulting in a six month or better average processing time for nearly all applications. To support the United States' humanitarian commitment, we have established a Refugee Corps that will provide a strong and effective overseas refugee-processing program able to fulfill the Refugee Affairs program's humanitarian objectives and more efficiently identify inadmissible people and those who are of national security interest.

We will work with the international trade community to facilitate and improve the flow of trade without compromising homeland security. The Automated Commercial Environment (ACE) will improve the Department's data-gathering capability, streamline filing processes, and reduce the paperwork burden by eliminating redundant filings required by Federal agencies. We will continue to use risk-assessment tools to more effectively allocate resources to allow maximum use of staffing and minimize customer inconvenience while ensuring adequate safeguards. To facilitate lawful travel and immigration, U.S. Customs and Border Protection will implement a new design of its facilities, starting in airports around the United States, to integrate the border functions and combine primary and secondary inspections into one. As a result, the majority of the traveling public will have less contact with Officers, allowing them to devote more time to those who are deemed higher risk. This will result in the better use of personnel, equipment and technology.

# Strategic Goal 7 Organizational Excellence

Value our most important resource, our people.  
Create a culture that promotes a common  
identity, innovation, mutual respect, account-  
ability and teamwork to achieve efficiencies,  
effectiveness and operational synergies.



## Serving the Public

The President's Management Agenda (PMA) provides a key framework for achieving organizational excellence. The Under Secretary for Management leads the overall improvement efforts to achieve the high standards of PMA in its targeted areas of improvement: Human Capital, Competitive Sourcing, Financial Performance, E-Government, Budget and Performance Integration, Faith-Based and Community Initiatives, and Real Property Management. A lead person in DHS headquarters is designated to develop and pursue plans for improvement in each area. This photo depicts a meeting of initiative area leads discussing plans to further advance progress to meet the President's high standards.

**I**n the spirit of the President's Management Agenda to improve management, and to fully achieve Organizational Excellence, we identified strategic objectives and established performance goals. For each performance goal, we developed quantitative performance measures with associated target levels of execution to measure our progress. These targets are used to derive the performance-based budget we submit to the Congress each year. Collectively, these measures are designed to achieve our strategic goal of Organizational Excellence. The table below correlates our Organizational Excellence objectives with the performance goals established for each objective, indicated by an objective number in the left hand column and the estimated net cost of efforts to achieve the objective. Also provided is information regarding the Department's performance as compared to our targets in FY 2006.





















STRATEGIC GOAL 7 - ORGANIZATIONAL EXCELLENCE			
STRATEGIC OBJECTIVES SUPPORTING GOAL 7			FY 06 Net Cost (in millions)
7.1 Value our people.			\$ 75.8
7.2 Drive toward a single departmental culture.			\$ 0
7.3 Continually improve our way of doing business.			\$ 627.5
<b>PERFORMANCE GOALS OF MAJOR PROGRAMS CONTRIBUTING TO OBJECTIVES</b>			<b>Detail on Page</b>
	7.3	Add value to the DHS programs and operations; ensure integrity of the DHS programs and operations; and enable the OIG to deliver quality products and services. (Audit, Inspections, and Investigations Program)	150
	7.3	The Department of Homeland Security components and stakeholders have world class information technology leadership and guidance enabling them to efficiently and effectively achieve their vision, mission and goals. (Office of the Chief Information Officer)	151
	7.3	Operating entities of the Department and other Federal agencies are promptly reimbursed for authorized unforeseen expenses arising from the prevention of or response to terrorist attacks. (Counterterrorism Fund)	151
	7.3	Provide comprehensive leadership, management, oversight, and support to improve the efficiency and effectiveness of the Department. (Office of the Secretary and Executive Management)	152
7.1	7.3	Improve the effective and efficient delivery of business and management services throughout the Department. (Office of the Under Secretary for Management)	152
	7.3	Develop and Maintain a Department-wide financial system that produces financial data that is timely, reliable, and useful to decision makers; strengthen accountability by ensuring that internal controls are in place across the Department and oversight reviews are conducted (Office of the Chief Financial Officer)	153

NOTE 1: The Net Cost measures the cost of supporting that entire strategic objective, not just the performance goal(s) identified in the table.

NOTE 2: The Secretary's Second Stage Review (2SR) was a major FY 2005 initiative. For FY 2006, additional measures were added in support of strategic objective 7.3. Some of these new measures indirectly support strategic objective 7.2.

## IMPLEMENTING THE PRESIDENT'S MANAGEMENT AGENDA

The *President's Management Agenda* was launched in August 2001 as a strategy for improving the management and performance of the Federal government. It focuses on the areas where deficiencies were most apparent and where the government could begin to deliver concrete, measurable results. The agenda includes five original initiatives: Strategic Management of Human Capital, Competitive Sourcing, Improved Financial Performance, Expanding Electronic Government, and Budget and Performance Integration. In addition to these initiatives, two new initiatives were subsequently added to the scorecard: Eliminating Improper Payments and Real Property. We have embraced the agenda since the Department was established in 2003 and have made steady progress each fiscal year. The Office of Management and Budget (OMB) regularly assesses our implementation of the agenda, issuing an Executive Branch Management Scorecard rating of green, yellow or red for both status and progress to achieve standards for each initiative. Overall, the Department improved in 2 of the status categories from last year's scorecard. The Department went from red to yellow in Eliminating Improper Payments and Real Property. The scorecard for the period ending September 30, 2006 rated the Department's status as green on zero (0) of the seven initiatives, yellow on 5 initiatives and red on the remaining 2. Progress scores were 4 green, 1 yellow and 2 red. Each year the standards for attaining green in the progress area are made more demanding. The Department continues to demonstrate progress in implementing government-wide program-specific initiatives. More detailed information regarding our progress may be found in the *Other Management Information, Initiatives, and Issues* section of this report, on page 72. A high level view of our progress, as rated by the scorecard is provided below.

PRESIDENT'S MANAGEMENT AGENDA SCORECARD				
(As of September 30, 2006)				
	Status			Progress
	FY04	FY05	FY06	FY06
Human Capital				
Competitive Sourcing				
Financial Performance				
E-Government				
Budget & Performance				
Eliminating Improper Payments *				
Real Property *				
* Program-Specific Initiatives				

A Department is "green" if it meets all of the standards for success, "yellow" if it has achieved some but not all of the criteria and "red" if it has even one of any number of serious flaws.



## HIGHLIGHTS

**S**ignificant accomplishments during fiscal year 2006 in achieving Organizational Excellence goals and objectives include the following:

**Expanded Electronic Government** — ensuring that the Federal government investment in information technology significantly improves the government's ability to serve citizens, and that information technology systems are secure and delivered on time and on budget; and

- Developed and successfully implemented an Enterprise Architecture (EA) to guide investment decisions and systems development activities for the department.
- Completed security certification and accreditation for 95 percent of the department's systems at the end of FY 2006, up from 35 percent at the beginning of the fiscal year.
- Complied with the FY 08 budget process requirement for identifying Federal Information Security Management Act (FISMA) systems that pertain to each major IT investment. Requiring that each FISMA system be mapped to an investment has resulted in a more accurate accounting for IT spending.
- Mapped all DHS IT investments to functional and IT portfolios, and developed portfolio cost reports.

**Real Property** – assuring that the Federal government's real property assets are available; of the right size and type; safe, secure and sustainable; able to provide quality workspaces; affordable; and operate efficiently and effectively.

- Developed the first accurate and current inventory of DHS real property assets. This inventory includes all installations, buildings, structures and land owned and operated in support of DHS missions.
- Published the DHS Asset Management Plan in June 2006.
- Established DHS-wide councils that provide management focus on real property across the Department and its components.

## FUTURE STEPS

**A**n agile and effective Department is essential to the rapid implementation of homeland security priorities, policies and objectives. We are establishing processes to identify and establish competitive standards and performance measures and, when appropriate, will recruit and retain the best people to provide effective and efficient services that ensure American citizens get the most value for their tax dollars. The Department will continue to communicate critical budget, cost and performance information to ensure stakeholders are informed, reasonable standards are set, and our people remain focused on getting the job done. We will maintain continual and unquestionable accountability and responsibility to ensure the effective use of resources allocated to the Department.

All elements of the Department will continue to ensure the core principles of organizational excellence are incorporated into our planning, programming and budgeting plans. During the next five years, our recapitalization efforts will include modernization that retains needed structure with enhanced capacity.

We will continue to work with our Federal, state, local and private-sector partners to invest in areas critical to achieving our mission, where our required capability is inadequate, performance is not competitive with alternative sources or where technology offers the prospect of decisive, transformational improvement in capability. Specific emphasis will be placed on eliminating systems where technology is obsolete or redundant, the usage rate is low, or the contribution to mission effectiveness is suspect or minimal. We are coordinating our workforce weaknesses and skill gaps with our eGov requirements and with our competitive sourcing schedules and opportunities. We will also continue implementing a unified, modern, performance-based personnel system and will educate and train homeland security professionals and our partners.

Significantly improved budget, performance and financial integration are key to the success of this effort. Managers must understand the full cost of their operations to the taxpayer and their level of competitive performance. This information will lead to better decision making in the allocation of resources as we work to move from periodic analysis to an ongoing project-by-project based capability.

## Analysis of Financial Statements

**T**hese financial statements are prepared in accordance with established Federal accounting standards and are audited by the independent accounting firm of KPMG LLP. It is the Department's goal to improve financial management and to provide accurate and reliable information that is useful for assessing performance and allocating resources. Figure 1 illustrates a condensed version of the Department's Consolidated Balance Sheet.

**Condensed Consolidated Balance Sheet**  
**As of September 30, 2006 and 2005**  
(In Millions)

	<b>FY 2006</b>	<b>FY 2005</b>	
	<b>(Unaudited)</b>	<b>(Unaudited)</b>	
		<b>(Restated)</b>	<b>Change</b>
<b>ASSETS</b>			
Intragovernmental Assets	\$63,773	\$101,048	\$(37,275)
Tax, Duties and Trade Receivables, Net	1,755	1,400	355
General Property, Plant and Equipment, Net	11,036	10,460	576
Other	2,669	1,588	1,081
<b>Total Assets</b>	<b>\$79,233</b>	<b>\$114,496</b>	<b>\$(35,263)</b>
<b>LIABILITIES</b>			
Intragovernmental Liabilities	\$21,665	\$3,135	\$18,530
Insurance Liabilities	3,567	23,433	(19,866)
Accrued Payroll and Benefits	1,362	1,366	(4)
Federal Employee and Veterans Benefits	32,278	30,050	2,228
Other	12,015	11,228	787
<b>Total Liabilities (Note 17)</b>	<b>\$70,887</b>	<b>\$69,212</b>	<b>\$1,675</b>
<b>Net Position</b>			
Unexpended Appropriations	48,102	87,131	(39,029)
Cumulative Results of Operations	(39,756)	(41,847)	2,091
<b>Total Net Position</b>	<b>\$8,346</b>	<b>\$45,284</b>	<b>\$(36,938)</b>
<b>Total Liabilities and Net Position</b>	<b>\$79,233</b>	<b>\$114,496</b>	<b>\$(35,263)</b>

Figure 1. Department's Consolidated Balance Sheet (Condensed)

### ASSETS

**I**n fiscal year 2006, the Department's assets totaled \$79,233 million. This is a decrease of \$35,263 million over the prior year's assets totaling \$114,496 million. The major portion of the decrease in Total Assets is in Intragovernmental Assets which is made up of primarily Fund Balance with Treasury and Advances and Prepayments. Intragovernmental Assets and General Property, Plant, and Equipment comprise 94% of total assets. Figure 2 summarizes the Department's assets as of September 30, 2006 and September 30, 2005.

Fund Balance with Treasury represents \$59,568 million or 93% of Intragovernmental Assets. The decrease in Intragovernmental Assets is due to a FEMA rescission, an increase in payments for Hurricane Katrina victims, and a reduction in the

amount of appropriations received by FEMA. A portion of Fund Balance with Treasury also includes Trust Funds, used to hold receipts for specific purposes; Revolving Funds, Liquidating and Working Capital Funds, used for continuing cycles of business-like activity; Special Funds, earmarked for specific purposes and Deposit Funds, amounts received as advances for which final disposition has not been determined. General Property, Plant and Equipment are primarily composed of aircraft, vessels, vehicles, land, structures, facilities, leasehold improvements, software, information technology, and other equipment that are used for general operations. Multi-use heritage assets consist primarily of buildings and structures owned by CBP and USCG.

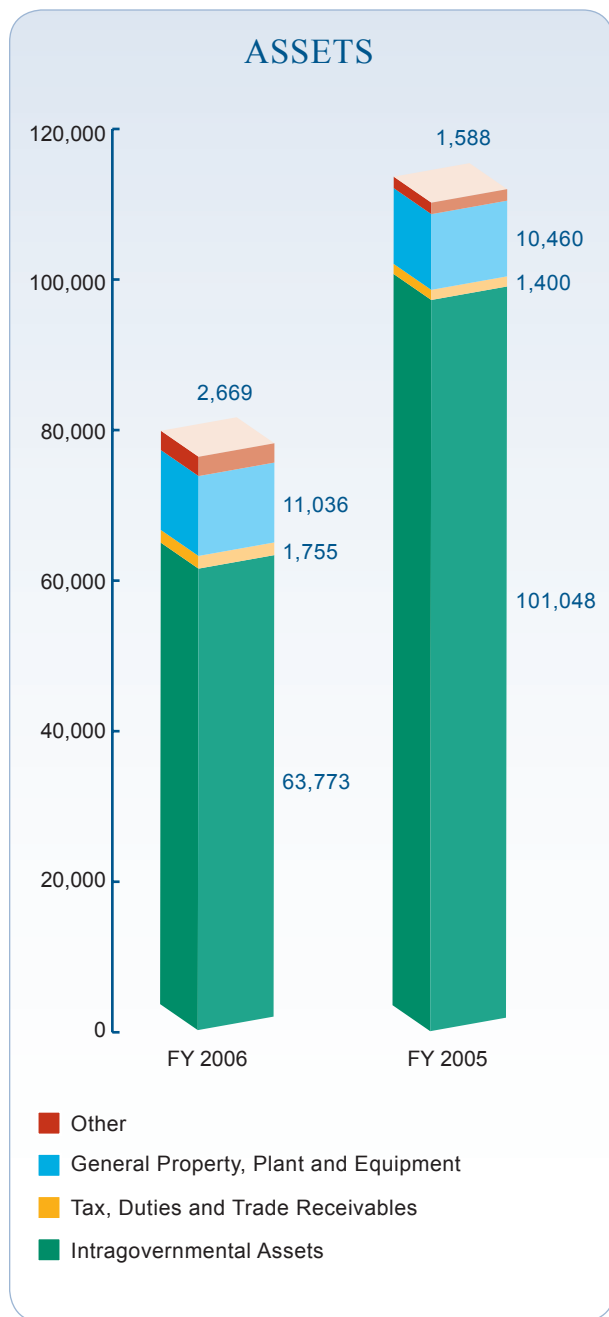


Figure 2. Department Assets

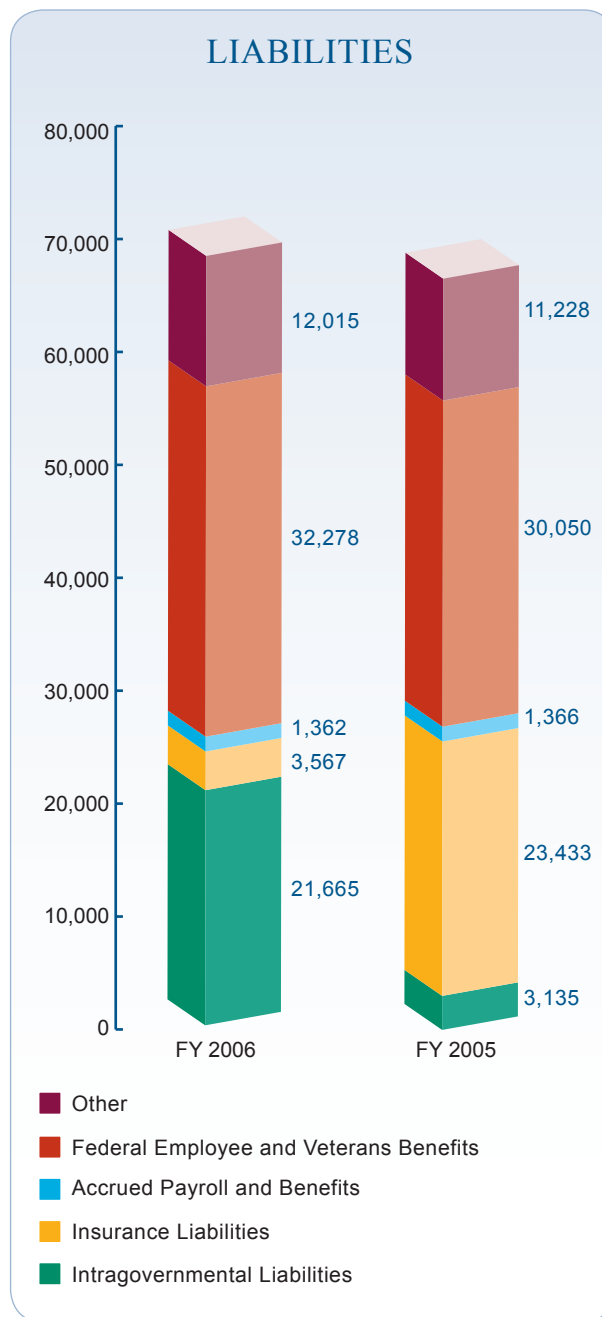


Figure 3. Department Liabilities

## LIABILITIES

**I**n fiscal year 2006, the Department's liabilities totaled \$70,887 million. This is an increase of \$1,675 million over the prior year's restated liabilities, which totaled \$69,212 million. Intragovernmental Liabilities is made up of primarily of debt to the U.S. Treasury, amounts due to the General Fund, and Accounts Payable. The difference in Intragovernmental Liabilities is due primarily to FEMA's increase in borrowings with the Bureau of Public Debt to cover claims settlements for Hurricane Katrina. The difference in Insurance Liabilities consists of FEMA payments of Hurricane Katrina claims.

Federal Employee and Veteran Benefits (arising primarily from U.S. Coast Guard personnel benefits) comprise 45% of the Department's total liabilities. *Figure 3* summarizes the Department's liabilities as of September 30, 2006, and September 30, 2005.

Federal agencies by law, cannot disburse money unless Congress has appropriated funds. Funded liabilities are expected to be paid from funds currently available to the Department. The Department's unfunded liabilities consist primarily of environmental and legal contingent liabilities and unfunded employee compensation costs, including FECA and annual leave. These liabilities will be paid from funds made available to the Department in future years. The associated expense is recognized in the period in which the liability is incurred.

## ENDING NET POSITION

**T**he Department's Net Position at the end of fiscal year 2006, disclosed in the Consolidated Balance Sheet and the Consolidated Statement of Changes in Net Position is made up primarily of two sections, Cumulative Results of Operations and Unexpended Appropriations. The total net position was \$8,346 million, a decrease of \$36,938 million from the previous year. The decrease is the result of a FEMA rescission.

## RESULTS OF OPERATIONS

**T**he Department's net cost of operations for fiscal year 2006 was \$54,318 million. This is a decrease of \$11,548 million from the previous year's restated net cost of \$65,866 million. The Department of Homeland Security Strategic Plan outlines the following mission goals: *Awareness, Prevention, Protection, Response, Recovery, Service, and Organizational Excellence*. Because of costs associated with Hurricane Katrina, FEMA Costs by Strategic Goals (Protection, Response, and Recovery) represent 43% of the Department's total net cost of operations. *Figure 4* illustrates a condensed version of the Department's Statement of Net Cost.

**Condensed Consolidated Statement of Net Costs**  
**For the Years Ended September 30, 2006 and 2005**  
(In Millions)

	FY 2006 (Unaudited)	FY 2005 (Unaudited) (Restated)	Change
<b>Cost by Directorate and Component</b>			
United States Visit	\$262	\$172	\$90
United States Customs and Border Protection	6,982	6,440	542
United States Coast Guard	9,587	8,925	662
United States Citizenship and Immigration Services	(120)	(347)	227
Federal Emergency Management Agency	23,217	37,484	(14,267)
Federal Law Enforcement Training Center	279	226	53
Preparedness Directorate	3,769	2,681	1,088
United States Immigration and Custom Enforcement	3,630	3,172	458
United States Secret Service	1,453	1,483	(30)
Science and Technology	843	731	112
Transportation Security Administration	3,566	4,268	(702)
Departmental Operations and Others	850	631	219
<b>Net Cost of Operations</b>	<u>\$54,318</u>	<u>\$65,866</u>	<u>\$(11,548)</u>
 Total Cost	 \$62,481	 \$73,479	 \$(10,998)
Total Revenue	(8,163)	(7,613)	(550)
<b>Net Cost of Operations</b>	<u>\$54,318</u>	<u>\$65,866</u>	<u>\$(11,548)</u>

Figure 4. Department's Statement of Net Cost (Condensed)

## REVENUES

**D**uring fiscal year 2006, the Department earned approximately \$8,163 million in revenues; this is an increase of about \$550 million from the restated amount of \$7,613 million on September 30, 2005.

The Department classifies revenues as either exchange or non-exchange revenue. Exchange revenues are those that derive from transactions in which both the government and the other party receive value, and that are directly related to departmental operations. The Department also collects non-exchange duties taxes and fee revenues on behalf of the Federal government. These are presented in the Statement of Custodial Activity rather than the Statement of Net Cost.

Examples of non-exchange revenues are user fees that CBP collects on behalf of the Federal Government as a result of its sovereign powers rather than as a result of providing goods or services for a fee. Donations to the Department are also reported as non-exchange revenues. Non-exchange revenues earned are either retained by the Department to further its mission or returned to the General Fund of the Treasury.

## CUSTODIAL ACTIVITY

In accordance with Federal accounting standards, revenues are presented in the Department's Statement of Custodial Activity since the collections are considered to be revenue of the Federal government as a whole rather than the Department. Revenues were \$23,564 million and \$27,580 million as of September 30, 2006 and 2005, respectively, and include duties, user fees, and excise taxes.

## BUDGETARY RESOURCES

The Department receives most of its funding from general government funds administered by the U.S. Treasury and appropriated for the Department's use by Congress. These resources consist of the balance at the beginning of the year, appropriations received during the year, and spending authority from offsetting collections as well as other sources of budgetary resources (Figure 5).

The Combined Statement of Budgetary Resources provides information on the budgetary resources that were made available to the Department for the year and the status of those resources at the end of the fiscal year. Obligations of \$91,412 million and \$68,628 million were incurred as of September 30, 2006 and 2005 on total budgetary resources of \$108,456 million and \$125,533 million, respectively (Figure 6). The Combined Statement of Budgetary Resources is presented on a combined basis rather than a consolidated basis for consistency with budget execution information and to properly report obligations incurred by the entire Department.

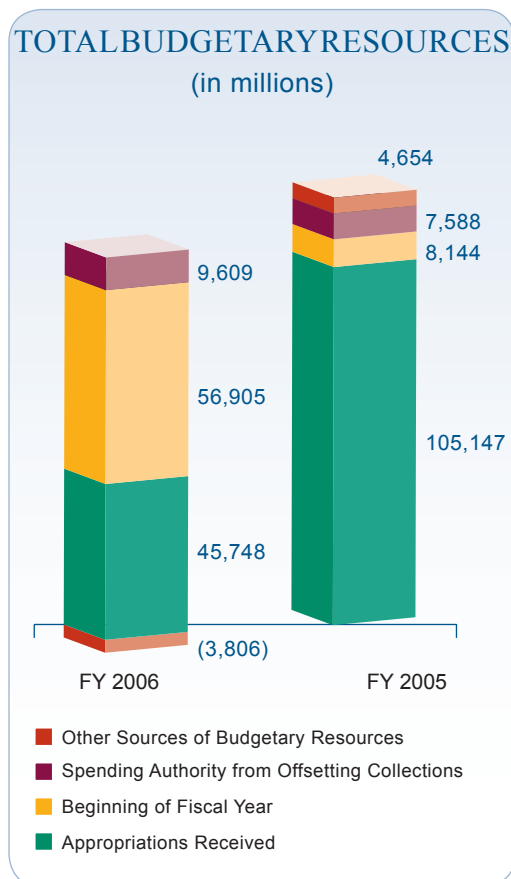


Figure 5. Total Budgetary Resources

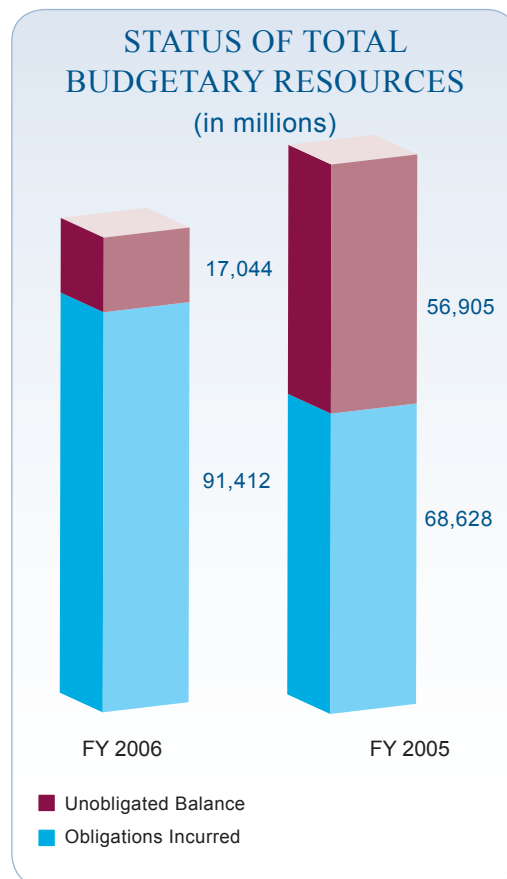


Figure 6. Status of Total Budgetary Resources



## ANALYSIS OF INTERNAL CONTROLS, SYSTEMS, AND LEGAL COMPLIANCE

### Federal Managers' Financial Integrity Act and the DHS Financial Accountability Act

DHS is responsible for establishing, maintaining, and assessing internal control to provide reasonable assurance that the control objectives of the Federal Managers' Financial Integrity Act, 31 U.S.C. 3512 Sections 2 and 4, are met and comply with applicable laws and regulations. To identify material weaknesses and non-conformance conditions, management used the following criteria:

- Merits the attention of the Executive Office of the President and the relevant Congressional oversight committees;
- Impairs fulfillment of essential operations or mission;
- Deprives the public of needed services;
- Significantly weakens established safeguards against waste, loss, unauthorized use or misappropriation of funds, property, other assets or conflicts of interest; and
- Financial management systems conformance to government-wide systems requirements.

In addition, the Department of Homeland Security Financial Accountability Act, P.L. 108-330, requires a separate assertion of internal control over financial reporting and an audit opinion of the Department's internal controls over its financial reporting. A material weakness pursuant to this Act is defined as a reportable condition or combination of reportable conditions, that results in more than a remote likelihood that a material misstatement of the financial statements or other significant financial reports, will not be prevented or detected.

The Department's Internal Control Committee (ICC) oversees the Department's internal control program. ICC membership includes a Senior Management Council (SMC), an Internal Control Coordination Board (ICCB), and a Senior Assessment Team (SAT). The SMC is comprised of the Department's Chief Financial Officer, Under Secretary for Management, Chief Administrative Services Officer, Chief Human Capital Officer, Chief Information Officer, Chief Information Security Officer, Chief Security Officer, and Chief Procurement Officer. The ICCB seeks to integrate and coordinate internal control assessments with other internal control related activities and includes representatives from all DHS lines of business to address crosscutting internal control issues. Finally, the SAT led by the Chief Financial Officer, is comprised of senior level financial managers assigned to carry out and direct component level internal control assessments.

Individual component assurance statements serve as the primary basis for the Secretary's Management Assurances. The assurance statements are based on information gathered from various sources including management initiated internal control assessments, program reviews, and evaluations. In addition, the Office of Inspector General and the Government Accountability Office conduct reviews, audits, inspections, and investigations.



# Homeland Security

## SECRETARY'S MANAGEMENT ASSURANCES

The Department of Homeland Security is committed to addressing the root causes of material weakness conditions and developing a culture of integrity, accountability, and excellence in all we do. The Department's management is responsible for establishing and maintaining effective internal control over the three internal control objectives of effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations. In addition, the safeguarding of assets is a subset of these objectives. In accordance with the Federal Managers' Financial Integrity Act and the Department of Homeland Security Financial Accountability Act, I have directed an evaluation of internal controls at the Department of Homeland Security in effect during the fiscal year ended September 30, 2006. This evaluation was conducted in accordance with OMB Circular No. A-123, *Management's Responsibility for Internal Control*, Revised December 21, 2004. Based on the results of this evaluation, the Department provides the following assurance statements.

### **Reporting Pursuant to the Federal Managers' Financial Integrity Act, Section 2 and the Department of Homeland Security Financial Accountability Act**

Based on information provided, the Department of Homeland Security provides reasonable assurance as to the overall adequacy and effectiveness of internal controls, except for internal controls over financial reporting as described in the paragraph below, and the following material weaknesses, as more specifically reported by the GAO High Risk Series:

- Implementing and Transforming the Department of Homeland Security;
- Establishing Appropriate and Effective Information-Sharing Mechanisms to Improve Homeland Security; and
- The National Flood Insurance Program.

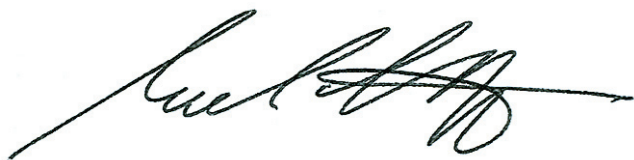
The Department of Homeland Security is unable to provide reasonable assurance that internal control over financial reporting was operating effectively. The following material weaknesses were found:

- Financial Management Oversight and Entity Level Controls;
- Financial Reporting Process;
- Financial System Security;
- Reconciling Fund Balances with Treasury;
- Accounting for Property, Plant, and Equipment;
- Accounting for Operating Materials and Supplies
- Accounting for Accounts and Grants Payable, and Legal Contingencies;
- Actuarial Liabilities;
- Budgetary Accounting and Undelivered Orders; and
- Reconciling Intragovernmental and Intradepartmental Balances.

**Reporting Pursuant to the Federal Managers' Financial Integrity Act, Section 4**

The Department of Homeland Security's financial management systems do not substantially conform to government-wide requirements. The following non-conformances were found:

- Federal Financial Management Systems Requirements;
- Federal Accounting Standards; and
- Noncompliance with the U.S. Standard General Ledger.

A handwritten signature in black ink, appearing to read 'Michael Chertoff', with a long horizontal stroke extending to the right.

Michael Chertoff  
Secretary Department of Homeland Security

Office of Inspector General


U.S. Department of Homeland Security  
Washington, DC 20528



**Homeland  
Security**

November 15, 2006

MEMORANDUM FOR: The Honorable Michael Chertoff  
Secretary

FROM:   
Richard L. Skinner  
Inspector General

SUBJECT: Independent Auditors' Report on DHS' FY 2006 Internal Controls  
over Financial Reporting

The attached report presents our independent auditors' opinion on internal controls over financial reporting as of September 30, 2006, based on the criteria established under the Federal Managers' Financial Integrity Act (FMFIA). DHS management is responsible for establishing and maintaining effective internal control over financial reporting. Our responsibility is to express an opinion on the effectiveness of DHS' internal control based on our examination.

The Department of Homeland Security Financial Accountability Act (The Act) (P.L. 108-330) was established to amend title 31 of the United States Code, to improve the financial accountability requirements applicable to the Department of Homeland Security (DHS). The Act also amended the Chief Financial Officers Act (CFO Act) of 1990 to include DHS as one of the federal agencies where the Chief Financial Officer is a Presidential appointee and reports directly to the Secretary.

Section 4 of The Act requires that the Secretary of Homeland Security include an audit opinion of the Department's internal controls over its financial reporting in each performance and accountability report beginning after fiscal year 2005.

We appreciate the cooperation extended to the auditors by DHS' financial offices. Should you have any questions, please call me, or your staff my contact David M. Zavada, Assistant Inspector General for Audits, at 202-254-4100.

Attachment

Office of Inspector General

U.S. Department of Homeland Security



**Homeland  
Security**

November 15, 2006

We have examined the effectiveness of DHS' internal control over financial reporting as of September 30, 2006 based on the criteria established under the Federal Managers' Financial Integrity Act (FMFIA). DHS management is responsible for establishing and maintaining effective internal control over financial reporting. Our responsibility is to express an opinion on the effectiveness of DHS' internal control based on our examination.

Our examination was conducted in accordance with U.S generally accepted government auditing standards. It included obtaining an understanding of the internal control over financial reporting and performing such other procedures as we considered necessary to render our opinion. We believe that our examination and the report of the independent auditor provide a reasonable basis for our opinion.


Because of inherent limitations in any internal control, misstatements due to error or fraud may occur and not be detected. Also, projections of any evaluation of the internal control over financial reporting to future periods are subject to the risk that the internal control may change, or that the degree of compliance with the policies or procedures may deteriorate.

During fiscal year 2006, the following reportable conditions were identified by an independent auditor, which are considered material weaknesses.

- Financial Management Oversight (Entity Level Controls);
- Financial Reporting;
- Financial Systems Security;
- Fund Balance with Treasury;
- Property, Plant and Equipment;
- Operating Materials and Supplies;
- Legal and Other Liabilities;
- Actuarial Liabilities;
- Budgetary Accounting; and
- Intragovernmental and Intradepartmental Balances.

A material weakness is a condition that precludes the entity's internal control from providing reasonable assurance that material misstatements in the financial statements will be prevented or detected on a timely basis. Due to the issues noted above, additional material weaknesses may exist that have not been reported.

Because of the effects of the above mentioned material weaknesses, in our opinion, DHS did not maintain effective internal control as of September 30, 2006, to meet the following objectives: (1) transactions are properly recorded, processed, and summarized to permit the preparation of the financial statements and stewardship information in conformity with GAAP, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition; and (2) transactions are executed in accordance with laws governing the use of budget authority and with other significant laws and regulations that could have a direct and material effect on the financial statements and stewardship information. Consequently, DHS' internal control did not provide reasonable assurance that misstatements, losses, or noncompliance material in relation to the financial statements or to stewardship information would be prevented or detected on a timely basis.



Richard L. Skinner  
Inspector General


U.S. Department of Homeland  
Security  
Washington, DC 20528



**Homeland  
Security**

**November 15, 2006**

**MEMORANDUM FOR:** Richard L. Skinner, Inspector General

**FROM:** David L. Norquist, Chief Financial Officer 

**SUBJECT:** Audit Opinion of the Department's Internal Controls over  
Financial Reporting

Thank you for the opportunity to review your draft audit opinion of the Department's internal controls over financial reporting. I agree with your draft audit report's conclusions and I am pleased that we have implemented the audit opinion requirement of the Department of Homeland Security Financial Accountability Act. I want to emphasize that I will continue to work with your office to ensure that inherited material weaknesses do not become ingrained into our operations. As we conclude the second year of implementing the Act, I appreciate our professional relationship and your office's efforts to establish an appropriate level of ongoing performance reporting that assesses and compliments management's corrective action efforts. The utility of your performance audits continues to develop through our combined efforts. I look forward to continuing this productive and successful relationship in FY 2007.



## GAO HIGH RISK AREAS

**D**HS' transformation was designated as a high risk area in FY 2003 because DHS had to transform 22 agencies into one Department and inherited a number of operational and management challenges from legacy components. In FY 2005, the GAO designated establishing appropriate and effective information sharing mechanisms as a high risk area to improve processes and procedures for partnering and coordinating efforts across the Federal government and within the private sector. In FY 2006, the GAO designated the National Flood Insurance Program as a high risk area due to the unprecedented magnitude and severity of flood losses resulting from hurricanes in FY 2005 and the extent to which the Federal government has exposure for flood claims coverage in catastrophic loss years.

DHS has made significant progress implementing the recommendations presented in GAO's updates; particularly in strategic planning, threat and risk assessments, financial management, information management, human capital and acquisition management. The Department will continue to strive for excellence in these areas. Progress in these areas is reported on in more detail within the related sections of Management's Response to the Office of the Inspector General's (OIG's) Reporting on Major Management Challenges section of the PAR.

## CORRECTIVE ACTION PLANS

**D**HS efforts in FY 2006 focused on strengthening corrective action plans and identifying areas where assurance can be provided. Most notably, the Department transformed its corrective action planning process to focus on identifying the root causes and issues underlying our pervasive weaknesses. The Department assessed the design of internal controls and prioritized plans to address internal control deficiencies by focusing on the elimination of pervasive material weaknesses. Over the past year, DHS has:

- Formalized the corrective action planning process through a Management Directive, guidance, and training.
- Implemented an automated corrective action tracking system to ensure progress is tracked and management is held accountable for progress.
- Developed a corrective action strategic planning process for improving financial management at DHS.
- Worked with the OMB to monitor corrective action plans.
- Established ongoing reporting by the DHS OIG that assesses and compliments management's corrective action efforts through performance audits.
- Executed the first phase of our OMB approved multi-year plan to implement a comprehensive internal control assessment pursuant to OMB Circular No. A-123 Appendix A, Management's Responsibility for Internal Control guidelines.

The following table presents a chart of Financial Audit Related Material Weaknesses, Reportable Conditions, and Noncompliance with Laws and Regulations by DHS from FY 2003 through FY 2006.

	FY 2003	FY 2004	FY 2005	FY 2006	FY 2006 Component Progress
<b>Material Weaknesses</b>	7	10	10	10	ICE, FEMA, GT, and DHS Components services by ICE
<b>Reportable Conditions</b>	7	3	2	2	CBP
<b>Noncompliance with Laws and Regulations</b>	3	4	7	8	
<b>Total</b>	17	17	19	20	

Although the Department's material weakness count remains at 10, significant progress was accomplished in FY 2006. Most notably, ICE eliminated pervasive material weakness conditions and was removed from six material weaknesses. In addition, ICE has made improvements for components for which they provide accounting services. This improvement was attributable to the leadership of the Assistant Secretary for ICE and the efforts of the ICE Chief Financial Officer to stabilize the control environment and focus on pervasive material weakness conditions. In addition, progress in implementing the DHS Financial Accountability Act continued with the Department's Chief Financial Officer's confirmation by the U.S. Senate. The increase in noncompliance with laws and regulations is attributable to a new finding related to the Debt Collection Improvement Act of 1996. The table below summarizes material weaknesses in internal controls as well as planned corrective actions with estimated target correction dates.

Material Weaknesses in Internal Controls Over Financial Reporting	DHS Component	Corrective Actions	Target Correction Date
<b>Financial Management Oversight and Entity Level Internal Controls:</b> DHS has not stabilized entity level controls related to the DHS control environment due to challenges surrounding the stand-up of the Department in FY 2003 and subsequent re-organizations in FY 2005 and FY 2006. Several key factors are needed to strengthen the control environment, including the development of human capital, cultural transformations, organizational structures, and financial management/oversight monitoring mechanisms. The Department is responsible for the establishment, maintenance, and assessment of internal controls to meet the objectives of the <i>Federal Managers' Financial Integrity Act</i> .	DHS OFM, USCG, and FEMA	The DHS OCFO will hire additional staff as suggested by the auditors and authorized by Congress. In addition, the OCFO will perform a study to identify additional training or organizational structure changes required. The Commandant of the USCG will lead a Financial Management Transformation Initiative designed to strengthen the USCG's financial management infrastructure. FEMA will coordinate corrective actions with the recent organizational changes mandated in the FY 2007 Homeland Security Appropriations Act, which combined FEMA and portions of the Preparedness Directorate.	FY 2009

Material Weaknesses in Internal Controls Over Financial Reporting	DHS Component	Corrective Actions	Target Correction Date
<p><b>Financial Reporting Process:</b> DHS has not established an effective financial reporting process due to limited staffing resources, informal policies and procedures, and lack of integrated financial processes and systems. The <i>Department of Homeland Security Financial Accountability Act</i> amended the <i>Chief Financial Officers Act</i> to include DHS as a CFO Act agency. As a result, DHS is required to submit to the Congress and OMB audited financial statements. Currently, due to pervasive material weakness conditions, DHS has engaged an independent auditor to perform a balance sheet and statement of custodial activity only audit.</p>	DHS OFM, USCG, and TSA	The DHS OCFO will develop comprehensive policies and procedures to establish effective Department-wide financial reporting control activities. USCG will improve policies and procedures surrounding account reconciliations and abnormal balances, and will implement Oracle system and process enhancements. TSA will improve policies and procedures for period end closings, and continue to work with the USCG to monitor and coordinate the resolution of financial reporting challenges.	FY 2010
<p><b>Financial Systems Security:</b> The Department's Independent Public Accountant had identified Financial Systems Security as a material weakness in internal controls since FY 2003 due to a myriad of inherited control deficiencies surrounding general computer and application controls. The <i>Federal Information Security Management Act</i> mandates that Federal Agencies maintain IT security programs in accordance with OMB and National Institute of Standards and Technology guidance.</p>	Department-wide	Additional financial audit support for DHS components will be provided from the Offices of the Chief Financial Officer and the Chief Information Security Officer in order to increase common FISMA and Federal Information System Controls Audit Manual (FISCAM) security control alignment based on: FIPS 199 Information Categories for Financial Reporting; POA&M reviews to ensure Component based Financial Audit Notice of Findings and Recommendations (NFRs) are being closed in a timely manner; General security control convergence based on NIST SP 800-53 and A-123 control categories for financially significant systems; Identified gaps between the A-123 requirements and existing DHS requirements (including NIST SP 800-53) and adjusting policy as appropriate; and Component OCFO C&A Review and Approval for all Financial Significant Systems.	FY 2008

Material Weaknesses in Internal Controls Over Financial Reporting	DHS Component	Corrective Actions	Target Correction Date
<b>Reconciling Fund Balance with Treasury:</b> USCG did not implement effective internal controls to accurately clear suspense transactions in order to perform accurate and timely reconciliations of Fund Balance with Treasury accounts.	USCG	USCG will develop policies and procedures for Fund Balance with Treasury (FBWT) which establish effective controls including monthly FBWT analyses, FBWT reconciliations, and suspense account clearing.	FY 2010
<b>Accounting for Property, Plant, and Equipment (PP&amp;E):</b> The controls and related processes surrounding USCG PP&E to accurately and consistently record PP&E are either not in place or contain errors and omissions. For example, physical inventory processes for PP&E and the methodologies and assumptions to support the total value of PP&E are not yet fully developed and implemented. Asset identification, mapping, and tagging are also areas of weakness within PP&E at the USCG. TSA has not implemented adequate policies and procedures to properly account for its property balances. The DHS OCFO and US-VISIT have not implemented policies and procedures to identify and account for software capitalization. As a result, DHS has not implemented SFFAS No. 6, <i>Accounting for Property, Plant, and Equipment</i> and SFFAS No. 10, <i>Accounting for Internal Use Software</i> .	USCG, TSA, and US-VISIT	USCG Property, Plant, and Equipment Corrective Actions are categorized into four categories: 1) In the area of repairable spares, USCG will centralize logistics management to a single set of policies and procedures, using a known CFO Act compliant business model to lower project risk and accelerate logistics transformation; 2) For real property management, USCG will transform the agency's real property data to the Department of Defense (DoD) methodology for classifying real property; 3) In the area of personal property, USCG will use inspection and assistance visits to units to validate internal control remediation efforts and suggest improvements in the design of controls to ensure units are making credible progress; and 4) For the Capital Investment Plan (CIP), the USCG will ensure complete policies are issued to support key assertions related to existence, completeness, and valuation for capitalized assets. US-VISIT, in conjunction with the DHS OCFO, will develop policies and procedures to account for software capitalization in accordance with SFFAS No. 10. The DHS OCFO will monitor corrective actions developed by TSA to address this new material weakness condition, within the first quarter of FY 2007.	FY 2010

Material Weaknesses in Internal Controls Over Financial Reporting	DHS Component	Corrective Actions	Target Correction Date
<p><b>Accounting for Operating Materials and Supplies:</b> Internal controls and related policies and procedures for physical inventory counts at USCG field locations have not been completely developed and implemented. As a result, DHS has not implemented SFFAS No. 3, <i>Accounting for Inventory and Related Property</i>.</p>	USCG	<p>The USCG will: centralize logistics management policies and procedures using a known CFO Act compliant business model to lower project risk; develop a requirements (maintenance) based allowance system; implement integrated financial and logistics technology to support the logistics business model; remove excess and obsolete material from field units to reduce the field held inventory footprint to a manageable level; and re-baseline unit inventory through the execution of wall to wall physical inventories and on-site management oversight.</p>	FY 2009
<p><b>Accounting for Accounts and Grants Payable, and Legal Contingencies:</b> Accounts payable and related obligations were identified as not complete, or recorded in an accurate and timely manner (including recording disbursements made by legacy agencies), and lacked proper approvals and supporting documentation. In addition, accrual methodologies were inconsistently applied and the monitoring of grant audits needs improvement in order to comply with the <i>Single Audit Act</i>. Finally, a scope limitation prevented the Independent Public Accountant from completing procedures for legal liabilities. As a result, DHS has not implemented SFFAS No. 1, <i>Accounting for Selected Assets and Liabilities</i>.</p>	DHS OFM, FEMA, G&T, TSA, and USCG	<p>The DHS OCFO will work with Components to develop policies and procedures for accounts payable and undelivered orders to ensure that the recording of obligations are complete, accurate, and timely with proper approvals and supporting documentation. The DHS OCFO will also develop policies and procedures to improve the legal liability reporting process. DHS Components will implement verification and validation procedures to ensure the quality of information. DHS Components will also consistently document accrual methodologies and monitor grant audits. FEMA will coordinate corrective actions with the recent organizational changes mandated in the FY 2007 Homeland Security Appropriations Act, which combined FEMA and portions of the Preparedness Directorate.</p>	FY 2009

Material Weaknesses in Internal Controls Over Financial Reporting	DHS Component	Corrective Actions	Target Correction Date
<b>Actuarial Liabilities:</b> USCG has not implemented effective internal controls over the accuracy of the data used to prepare the calculations surrounding the actuarial pension liability, post employment medical liability and the post employment travel benefit liability. As a result, DHS has not implemented SFFAS No. 5, <i>Accounting for Liabilities of the Federal Government</i> .	USCG	USCG will implement a unified financial management system (Core Accounting System) to improve the accuracy and completeness of the underlying participant human resource data provided to the actuary. In addition, USCG will develop sufficient financial and human capital resources, trained with the correct skill sets and competencies, including financial management, to properly manage pension and medical accounts.	FY 2009
<b>Budgetary Accounting and Undelivered Orders:</b> Accounts payable and obligations were identified as not recorded accurately and timely in the financial systems of DHS Components, which could lead to non-compliance with laws and regulations such as the <i>Anti-Deficiency Act</i> . Specifically, there is a need for overall improved recording, monitoring, reporting, and close outs over all DHS obligations and reconciling budgetary vs. proprietary account relationships.	ICE, USCG, TSA, FEMA, US-VISIT, and DHS MGMT	The DHS OCFO will work with Components to develop policies and procedures for budgetary accounting which allow DHS financial management personnel to establish effective controls and properly record and close out obligations. DHS Components will ensure that obligations are recorded and reconciled in an accurate and timely manner and supported with proper documentation.	FY 2009

Material Weaknesses in Internal Controls Over Financial Reporting	DHS Component	Corrective Actions	Target Correction Date
<p><b>Reconciling Intragovernmental and Intradepartmental Balances:</b> DHS and Components have not fully implemented policies and procedures to routinely identify and reconcile intragovernmental and intradepartmental balances and transactions with trading partners to ensure balances properly eliminate in the government-wide and DHS consolidated financial statements.</p>	DHS OFM	<p>The DHS OCFO will issue policies and procedures to establish clear roles and responsibilities that allow DHS Component financial management personnel to establish effective controls over governmental transaction accounting and reporting. These policies and procedures will address development of a four digit trading partner to ALC crosswalk, timely dissemination of FMS elimination updates and ranking and reaching out to the largest trading partners and sharing usage reports by agreement. Further, regular training for procurement staff handling inter-governmental agreements as well as accounting staff maintaining vendor table data will be developed. The DHS OCFO will dedicate additional resources to assist the components in the reconciliation process. Finally, when all other outlets have been exhausted, there must be a process implemented for timely CFO to CFO communications to resolve material discrepancies and/or CFO Council support for resolving inter-agency trading partner issues.</p>	FY 2009



## FEDERAL FINANCIAL MANAGEMENT IMPROVEMENT ACT

**T**he Federal Financial Management Improvement Act of 1996 (FFMIA) requires Federal agencies to implement and maintain financial management systems that comply substantially with: (1) Federal financial management system requirements, (2) applicable Federal accounting standards, and (3) the U.S. Standard General Ledger at the transaction level. In assessing compliance with FFMIA, DHS utilizes OMB guidance and considers the results of the OIG, annual financial statement audits, and Federal Information Security Management Act (FISMA) compliance reviews. As reported in the Secretary's Management Assurance Statements, DHS financial management systems do not substantially conform to government-wide requirements, however, significant progress has been made to certify and accredit all financial management systems in accordance with the FISMA.

### Financial Systems Framework

**Department-wide Initiatives:** On September 13, 2006, the Department's CFO testified before Congress that DHS' goals for improving its financial systems have not changed and a major effort remains to improve all of its resource management systems. Rather than focus only on systems, the CFO is currently developing an overarching strategy to address challenges in the areas of people, process, policy, and assurances to achieve the Department's goals of obtaining a clean audit opinion, establishing sound internal controls, and improving the efficiency of financial operations. DHS understands that some systems are aging; that some fail to meet all user requirements; and that some are not fully integrated with finance, procurement, logistics, and asset management. To meet these needs, rather than acquiring, configuring, and implementing a new system within DHS, we are planning to fully leverage investments that have already been made in people, process, and systems. Migration is only one component of an improvement program and can be costly and risky, takes time and effort, and is very disruptive. Consequently, no migrations will be considered unless: 1) DHS knows that a system is a root cause of a problem, and 2) the benefits of a migration outweigh the costs. Before DHS makes any migrations, major upgrades, or consolidations, DHS will prepare a business case that assesses the impacts and benefits. Currently, DHS is completing a business case and is compiling the information necessary to assess the quality of its systems, using, in part, work done in past audits, as well as reviews performed under **eMerge**<sup>2</sup>.

The DHS plan looks beyond immediate systems improvements to include the strengthening of internal controls. Based on OMB's Circular A-127, *Financial Management Systems* guidance and the objectives of FFMIA, DHS plans to strengthen the integration of internal control over financial reporting process level assessments by addressing process, people, policy, and system problems concurrently and collaboratively to ensure improvements are made effectively. An initial triage will be conducted over the next several months to determine which systems today meet the basic standards for financial management and which can meet standards with modest improvement. We will look to leverage these systems first as solutions for those components currently using systems that fail to meet standards. Once the systems triage has been completed, we will employ, on an ongoing basis, a combined process and system approach to monitor status and to assess progress made on corrective action plans. We will use performance metrics and ongoing operational analyses, in conjunction with a business case, to determine whether to continue, improve, or discontinue supporting systems.

DHS will use an integrated project team approach to design and implement internal controls and to improve the effectiveness and efficiency of financial operations, leveraging the process designs created during the first phase of the **eMerge**<sup>2</sup> program as the framework of change. The framework integrates people, process, policy, system, and assurance activities and ensures that systems capabilities are fully leveraged in establishing controls and in improving operations.

The CFO will leverage other opportunities to improve systems, such as organizational changes, major lifecycle milestones, and findings and recommendations from ongoing operational analyses.

**CBP:** As part of CBP's continuing efforts to modernize its financial systems, an Enterprise Resource Planning (ERP) system solution, Systems, Applications and Products (SAP) was successfully implemented. CBP is now beginning its third year of operation using SAP and deriving the expected benefits. SAP provides the tools for enhanced customer service and facilitates a shift in the role of finance from a transaction process/record-keeping function to a more analytical and integrated decision-making function. CBP utilizes SAP as an integrated solution for its Budget, Procurement, Asset Management, Finance, and Reporting business processes. This system gives CBP a state-of-the-art, fully integrated system in which to plan, acquire, track and fully account for all purchases and assets, as well as track budgets and provide management with timely and accurate financial reports.

The future holds many prospects for expanding and improving the SAP system at CBP. New systems being planned for and developed will be interfaced, such as the CBP future eTravel system. These plans cannot exclude continued efforts to build on the momentum the CBP Modernization Office has created in developing SAP as a core revenue accounting system for the Automated Commercial Environment (ACE). Many successes have been realized by the implementation of SAP at CBP, and more will be accomplished. All of these tasks will be completed as efficiently and timely as they have in the past in order to continue to enable the CBP frontline to accomplish their goals of fighting terrorism and safeguarding the American homeland.

**FLETC:** In May 2006, the FLETC awarded a multi-year contract for the development and implementation of the Student Administration Scheduling System (SASS). The SASS will replace the antiquated Student Information System (SIS) and will integrate the FLETC's numerous manual and partially automated processes in training administration. The SASS will also enable the FLETC to apply standardized scheduling priorities enterprise-wide and to thoroughly analyze all aspects of program and facility scheduling, as well as student administration functions. These tools will provide information necessary to efficiently utilize current resources, plan for future requirements, and more effectively respond to the training needs of the FLETC's partner organizations. As with the SIS, the SASS data on student and course attendance are essential billing information that will be uploaded via an interface to the financial management system.

**TSA:** At the beginning of FY 2005, TSA migrated its financial management operations from the Department of Transportation (DoT) financial management systems environment to the USCG financial systems environment. USCG's suite of financial systems includes the Core Accounting System (Oracle Federal Financials 11.5.9), Finance and Procurement Desktop (a front-end tool that enables program and field office personnel to execute requisitions and track spending online), Markview invoice imaging and routing system, and Sunflower Asset Management System. The migration has reduced the Department's dependency on an external department, brought the financial management activities of two of the Department's largest components under one roof, and is expected to generate economies of scale as both TSA and USCG will realize benefits from future investments in system upgrades.

Following up on the successful financial systems transition, both TSA and the USCG migrated its payroll processing function from DOT to the U.S. Department of Agriculture's National Finance Center (NFC) systems in August 2005. This transition put TSA on the same payroll platform as all other Components and has resulted in more efficient payroll services for TSA employees. An interface from NFC to the Core Accounting System ensures that payroll costs are accurately accounted for in the general ledger.

In FY 2006, TSA continued its efforts to improve financial management and systems through the increased use of the Contract Information Management System (CIMS). CIMS, an adaptation of the widely used PRISM software, is gradually replacing TSA's current manual contract writing process. In addition to easing the administrative burden of developing government contracts, CIMS interfaces with the Core Accounting System to liquidate commitments and post obligations; processes that in the past have required manual data entry.

TSA's efforts to improve financial management and systems will continue in FY 2007. TSA's focus will be on correcting

financial system weaknesses previously identified by auditors. New system capabilities will be implemented to strengthen funds control.

**ICE:** In March 2006, the ICE CFO and CIO agreed to transfer technical responsibilities for the Federal Financial Management System (FFMS) and Travel Management System (TMS) from the ICE Office of Financial Management to the ICE Chief Information Officer. The transition placed the responsibility for system performance and maintenance under the auspices of the OCIO. Since that transfer, the payroll and travel manager financial system interfaces were rewritten to substantially decrease the amount of time required to process transactions. Additionally, a major effort went into fine tuning reports and stabilizing report servers.

PRISM continues to be in use throughout all ICE procurement offices. During FY 2006, an interface to FFMS was designed, developed, and accepted. It is currently on hold for deployment awaiting DHS OCIO re-hosting of PRISM.

## FEDERAL INFORMATION SECURITY MANAGEMENT ACT

**T**he E-Government Act of 2002 (Public Law 107-347) Title III FISMA provided a framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets. FISMA introduced a statutory definition for information security. The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. In addition, the House Appropriations Committee (HAC) Report 109-079, Department of Homeland Security 2006 Appropriations Bill, directed the "Department's CIO to develop a plan to address the weaknesses in DHS' information security" by October 1, 2005. The committee report identified four weaknesses in the information security program. In FY 2006, the Department completed a number of improvements which have significantly improved DHS information system security compliance.

### Policy and Guidance

A number of updates to the DHS Information Security policy directives (DHS MD 4300A) were issued over the past year, with the latest Version 4.2 dated September 29, 2006, published on the DHS intranet Web site at <https://dhsonline.dh.gov/portal/>. Since October 2005, policies have been added and updated to address: Contingency Planning, Remote Access, Personally Identifiable Information, Wireless, IPV6, and Incident Reporting.

The DHS security architecture design guidance Volumes 1, 2, and 3 were also updated this past year and distributed to all HQ and component Information System Security Managers (ISSMs) and Information System Security Officers (ISSOs).

In May 2006, DHS updated agency-wide security configuration policies based on updated hardening configuration guides for Windows 95, Windows XP Professional, Windows NT, Windows 2000 Professional, Windows 2000 Server, Windows 2003 Server, Solaris, HP-UX, Linux, Cisco IOS Routers, Oracle, and SQL Servers.

### Tools and Processes

The Department implemented two enterprise tools to facilitate agency-wide security management and compliance:

- FISMA Tracking Tool, and
- Risk Management Control Tool.

These two information security tools were deployed across DHS starting in April 2005 and the use of these tools was mandated by DHS 4300A Policy and Handbook for all sensitive systems. The automated risk management tool is the basis

for Certification and Accreditation (C&A) compliance with policy for management, operational, and technical controls. The FISMA tool tracks eleven documents mandated for C&A based on NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. FISMA artifacts were also tracked for inventory management, self-assessments, FIPS199 security categorization, privacy threshold assessments, e-authentication assessments, and interconnect security agreements. Extensive training on the C&A process and the use of these tools was provided to DHS ISSMs and ISSOs throughout the year and at the Department's annual security conference.

The Office of Information Security updated the processes supporting Plans of Actions and Milestones (POA&Ms). POA&Ms are used to identify and prioritize security weaknesses at system, program, or departmental levels for remediation. DHS conducted component site visits and provided POA&M training to increase the quality and completeness of POA&M data.

DHS processes were implemented that more effectively tie OMB Exhibit 300s OCIO and CFO portfolios to DHS information system accreditation.

### Information System Inventory

In FY 2005, DHS completed a comprehensive inventory of its sensitive but unclassified systems including agency and contractor systems. The inventory consists of general support systems (GSSs) and major applications (MAs). In the DHS FY 2006 FISMA Report, 692 IT Systems were identified. The DHS inventory is under strict change control. Any additions, deletions or changes to the inventory are tracked to ensure accuracy.

### Certification and Accreditation of Information Systems

The Department's C&A Tool was used to collect Department-wide remediation progress data for C&As across the DHS inventory. DHS certified and accredited 95% of its operational systems by the end of FY 2006, as illustrated in the following figure.

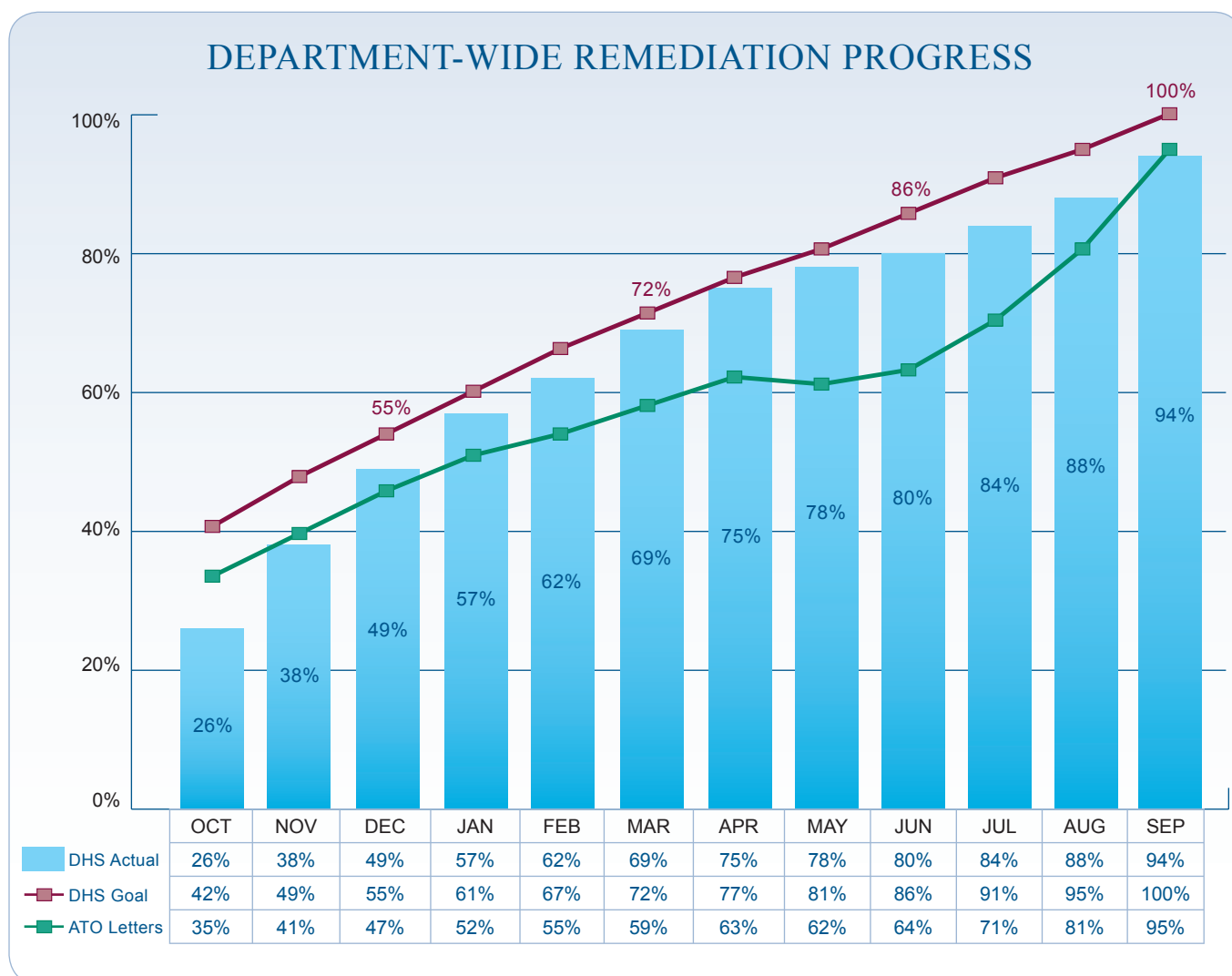


Figure 7. DHS Certification and Accreditation Progress – FY 2006

The DHS Information Security Performance Plan for FY 2007 is to continue “Raising the Bar” on the Department’s information security posture, particularly in the following areas:

- Maintaining a steady state of system C&A’s;
- Raising the quality of the C&A artifacts;
- Increasing support for annual testing of information security controls;
- Providing increased emphasis to close high priority POA&Ms;
- Improving the quality of configuration management processes and reporting;
- Increasing the consistency of incident detection and response reporting; and
- Continuing information security training.

Additional financial audit support for DHS components will be provided from the Offices of the Chief Financial Officer and the Chief Information Security Officer in order to increase common FISMA and Federal Information System Controls Audit Manual (FISCAM) security control alignment based on:

- FIPS 199 Information Categories for Financial Reporting
- POA&M reviews to ensure Component based Financial Audit Notice of Findings and Recommendations (NFRs) are being

closed in a timely manner.

- General security control convergence based on NIST SP 800-53 and A-123 control categories for financially significant systems.
- Identified gaps between the A-123 requirements and existing DHS requirements (including NIST SP 800-53) and adjusting policy as appropriate.
- Component OCFO C&A Review and Approval for all Financial Significant Systems.

## IMPROPER PAYMENTS INFORMATION ACT

DHS' improper payments work was dominated by FEMA's examination of Hurricane Katrina disaster relief fund payments. These payments were issued in unprecedented quantities under the most challenging of conditions. FEMA management performed extensive sample payment testing to meet Improper Payments Information Act (IPIA) requirements, to satisfy Congressional inquiries, and to complete an assessment of key internal controls. This testing conclusively showed that FEMA's disaster relief funds are at high risk for issuing improper payments. Testing of Individuals and Household's Program payments yielded an estimated improper payment amount of \$450 million or 8.56% of \$5.25 billion disbursed between September 1, 2005 and March 1, 2006. FEMA's test results varied from GAO report No. GAO-06-844T for the Individuals and Households Program which estimated the error rate at 16% and the error total between \$600 million and \$1.4 billion. Testing of disaster relief fund vendor payments yielded an estimated improper payment amount of \$319 million or 7.44% of \$4.29 billion disbursed between September 1, 2005 and March 1, 2006. For full details, see the IPIA Reporting Details Section of Other Accompanying Information.

FEMA management has already begun to address many internal control deficiencies identified in Government Accounting Office and Inspector General reports and in its own internal control assessment. FEMA management will complete a corrective action plan to reduce improper payments, establish internal controls which are operating effectively, and recoup monies paid in error or due to fraud.

In FY 2006, DHS continued to improve IPIA procedures. Last year, the Department defined IPIA programs by using Treasury Appropriation Fund Symbols (TAFS). This year, the Department worked with Components to group TAFS into readily identifiable IPIA programs. Payment sample testing was expanded from FY 2005's testing of the largest TAFS at each component to the testing of all IPIA Programs with more than \$100 million in relevant disbursements. A statistical team was utilized to design payment sample test plans that would yield significant results per OMB guidance. This statistical team extrapolated results for programs which could exceed the OMB high risk reporting ceilings.

Improper payments testing at CBP, FLETC, ICE, TSA, USCG, and USSS identified that improper payments had been issued but not at rates and amounts exceeding OMB's high risk thresholds. GT did not complete payment sample testing; FEMA did not test non-Disaster payments or non-Katrina Disaster payments; and the USCG did not test FAMS. It is not known whether these programs are at high risk for issuing improper payments.

In addition to management's payment sample testing, the Department is working to establish an effective secondary control by having recovery audit work performed at CBP, ICE, and USCG. This recovery audit work has progressed throughout the year but is not at a point to yield conclusive summary results. Reports to date, however, are consistent with the not at high risk determination which came from management's payment sample testing at these components.

## OTHER KEY LEGAL AND REGULATORY REQUIREMENTS

### Prompt Payment Act

The Prompt Payment Act requires Federal agencies to make timely payments (within 30 days of receipt of invoice) to vendors for supplies and services, to pay interest penalties when payments are made after the due date, and to take cash discounts only when they are economically justified. The Department's components submit Prompt Payment data as part of data gathered for the CFO Council's Measurement Tracking System (MTS). Periodic reviews are conducted by the components to identify potential problems. Interest penalties as a percentage of the dollar amount of invoices subject to the Prompt Payment Act has remained below 0.1% throughout the August 2005 – August 2006 period that the statistics have been kept (MTS statistics are reported with a six week lag).

### Debt Collection Improvement Act (DCIA)

The DHS OCFO is in the process of developing and implementing comprehensive debt collection regulations that would end the components reliance on legacy agency regulations. The DHS-wide debt collection regulations will provide instructions to the components on meeting the reporting requirements in support of the Debt Collection Improvement Act of 1996 (DCIA). This act established the following purposes:

- To maximize collections of delinquent debts owed to the Federal Government by ensuring quick action to enforce recovery of debts and the use of all appropriate collection tools.
- To minimize the costs of debt collection by consolidating related functions and activities and utilizing interagency teams.
- To reduce losses arising from debt management activities by requiring proper screening of potential borrowers, aggressive monitoring of all accounts, and sharing of information within and among Federal agencies.
- To ensure that the public is fully informed of the Federal Government's debt collection policies and that debtors are cognizant of their financial obligations to repay amounts owed to the Federal Government.
- To ensure that debtors have appropriate due process rights, including the ability to verify, challenge, and compromise claims, and access to administrative appeals procedures which are both reasonable and protect the interests of the United States.
- To encourage agencies, when appropriate, to sell delinquent debt, particularly debts with underlying collateral.
- To rely on the experience and expertise of private sector professionals to provide debt collection services to DHS components.

To achieve these purposes, the Department's goals are to: (1) overcome DCIA deficiencies by having a fair and aggressive program to recover delinquent debt, (2) improve the Department's debt collection performance by promoting the resolution of delinquencies as quickly as possible, and (3) reduce future write-offs of debt by implementing a debt collection strategy, consistent with government-wide and agency requirements, to restore the delinquent debts to current status or, if unsuccessful, maximize collections.

### FY 2006 Biennial User Charges Review

The Chief Financial Officers Act of 1990 requires each agency CFO to review, on a biennial basis, the fees, royalties, rents and other charges imposed by the agency, for services and things of value provided to specific recipients, beyond those received by the general public. The purpose of these reviews is to identify those agencies assessing user fees, and to periodically adjust existing charges to: (1) reflect unanticipated changes in costs or market values; and (2) to review all other agency programs to determine whether fees should be assessed for government services or the use of government goods or services.



A preliminary review of DHS user fees was conducted by the OCFO in FY 2006. This review was based on component FY 2005 data and user fee structures that had been established through the legacy agencies. The review indicates that: (1) changes in statutes and regulations are needed to consolidate some CBP user fee programs; (2) a review of user fee rates is necessary to ensure full allowable costs are being recovered for goods and services provided by CBP and TSA; and (3) the collection and management of user charges need to be simplified, for all components, as a natural progression of the DHS "one face at the border" initiative. The DHS components will continue striving to improve the methodology for a DHS-wide user fee delivery model and seek opportunities to consolidate revenue collection where necessary.

To ensure compliance with this biennial requirement, each DHS component is required to compile and furnish individual summaries for each user fee by addressing the key points for each user fee, in sufficient detail, to facilitate a review by the OCFO. For FY 2005, five DHS components were responsible for collecting forty-eight different user fees covering various services provided to the traveling public and trade community. The following is a detailed analysis of the fee collections and costs of the related services:

- **CBP:** The user fee programs for CBP consist of 38 different fees covering various services provided to passengers and conveyances at ports of entry to the United States. In FY 2005, the fees collection totaled \$1.042 billion and the costs for services provided relative to these fees totaled \$1.676 billion. The shortfall from fee revenue is over \$634 million. A proposed user fee initiative by the CBP would consolidate all user fees that fund CBP inspections and would unify administrative and fee setting authority among the different fees. These changes will result in significant savings to the component and recipient.
- **USCIS:** USCIS is responsible for collecting fees from persons requesting immigration benefits and depositing them into the Immigration Examination Fee Account (IEFA). These fees are used to fund the full cost of processing immigration and naturalization benefit applications and petitions, biometric services, and associated support services. In addition, these fees must recover the cost of providing similar services to asylum and refugee applicants and certain other immigrants at no charge. The IEFA fees generated a total of \$1.533 billion in revenues and \$1.510 billion in expenditures resulting in a surplus of \$23 million. USCIS is currently conducting a new comprehensive review of the resources and activities funded by the IEFA to determine whether the current fees reflect current processes and recover the full costs of services provided.
- **TSA:** TSA is responsible for collecting five different security fees which include: the September 11th Security Fee, the Aviation Security Infrastructure Fee, Fees for Security Threat Assessments for HAZMAT Drivers, Flight Training for Aliens Fee, and the Ronald Reagan Washington National Airport Enhanced Security Procedures for Certain Operations Fees. During FY 2005, TSA collected \$2.212 billion for these five fees. The obligations incurred by TSA for providing these services were \$4.104 billion. This amount exceeded related fee collections by \$1.892 billion.
- **USCG:** The Omnibus Budget Reconciliation Act of 1990 amended 46 U.S.C 2110, removed long-standing prohibitions against charging direct user fees for services provided to commercial vessels and maritime personnel and required the USCG to charge fees for the following services: (1) Merchant Mariner Licensing and Documentation User Fees, (2) Commercial and Recreational Vessel Documentation User Fees, and (3) Vessel Inspection User Fees for U.S. and foreign vessels requiring a certificate of inspection. In FY 2005, the fee collections from these services amounted to \$24.8 million.
- **ICE:** ICE collects fees for the Student Exchange and Visitor Program (SEVP) School Certification and the Student and Exchange Visitor Information System (SEVIS). These programs provide a mechanism for monitoring and providing information on student and exchange visitor status violators. In FY 2005, the fees collected for these two programs totaled \$46.5 million. In addition, Immigration User Fees totaling \$100.5 million were collected by CBP on behalf of ICE and transferred to an Appropriated Earmarked Receipts Account during FY 2005.

## Other Management Information, Initiatives, and Issues

While this report focuses on the Department's performance goals, measures and financial performance, we also strived to improve every aspect of management of this large and complex organization. The cornerstone of that effort was the President's Management Agenda, under which the Department's management achieved wide-ranging success throughout fiscal year 2006. This section expands upon the highlights presented in the performance section on Organizational Excellence. To see the performance goal results, please refer back to that section.

### SUCSESSESS UNDER THE PRESIDENTS MANAGEMENT AGENDA

**Strategic Management of Human Capital** - having processes in place to ensure the right person is in the right job, at the right time, and is not only performing, but performing well.

- To ensure a pipeline for leadership positions, the Department developed and received approval of a DHS Succession Management Plan, which requires the review of leadership needs based on strategic and program plans, the identification of sources of key talent, and the assessment and management of the identified talent. The Department has also announced its first SES Candidate Development Program and has begun evaluating applications.
- The Department made considerable progress in implementing MAXHR, the new performance-based human resources management system. The MAXHR Performance Management Program, including the online ePerformance Tool, has been designed and is now deployed to more than 5,000 employees in Headquarters, the U.S. Coast Guard, Immigration and Customs Enforcement, and the Federal Law Enforcement Training Center. By the end of 2006, coverage will expand to Citizenship and Immigration Services and Customs and Border Protection, bringing the total number of employees covered by MAXHR to approximately 11,000. To date, 350 senior executives and more than 11,000 managers and supervisors have received formal training in performance leadership. In addition, Components have also participated in "goal alignment" sessions to ensure that individual performance goals align with the strategic priorities of the organization.
- To allow employees and managers to focus on crucial missions, the Department continued aggressive initiatives to minimize the time and effort that employees expend in administrative activities. Notably, the Department became the first agency to convert to Electronic Official Personnel Files (e-OPF); converting literally tons of paper personnel files into digitized format that employees easily access online via the web. DHS worked with OPM on this eGov initiative serving as a model for other government agencies. Additionally the Department continued implementing a new web-based time and attendance system "webTA"; this past year Headquarters and the US Secret Service joined other components and by going live, bringing the total number of covered employees to almost 80,000. This system reduces the manual labor dependency of processing paper timesheets; instead, time and leave requests and approvals can be processed online via one intuitive web-based system.
- DHS developed and received approval of its Human Capital Accountability System which will provide regular evaluation of human resources management. The system is designed to ensure that HC programs across the Department are aligned with mission and goals, are in compliance with merit system principles, law, and regulation, and are efficiently and effectively implemented. In FY 2006, a total of 18 audits of human resources operations and/or delegated examining units were conducted by OPM and the Department; corrective actions were identified and have, or are being addressed by the responsible offices.

- The Department submitted a comprehensive Human Resources Professional Improvement Plan to OPM/OMB. DHS combined the nine competencies identified in the government-wide CHCO Council Competency Model with additional competencies identified in research to develop a DHS Competency Model. Based on an assessment of the current workforce, a plan was developed to close the competency gaps. Therefore the HRM Improvement Plan was developed based on the DHS Competency Model and the following four major roles for HR Specialists: Technical Expert, Change Consultant, Strategic Partner, and Coach/Mentor.

**Competitive Sourcing** — competitively examining commercially available mission and support services to determine whether it is more effective to obtain such services from Federal employees, under reimbursable agreements with other Federal agencies or from the private sector;

- The Department made considerable progress in expanding the learning curve, scope and the number of completed OMB Circular A-76 competitions in FY 06 and, based on that experience, approved a revised Green Plan for conducting future competitions that expects to compete over 18,000 FTE. Five Streamlined and two Standard competitions were completed in FY 06, bringing the total number of completed competitions since 2003 to seventeen. Over 500 in-house FTE have now been involved in these competitions. More importantly, the Department expanded the scope of the program to include more Components and apply a wider range of functions to the dynamics of competition with associated performance and cost metrics.
- The Department completed the first Tri-Bureau competition of its language translation function, involving FTE from CIS, CBP and ICE. This competition facilitated the restructuring of legacy agency support involving over 100 different language requirements.
- The USCG completed its Civil Engineering Unit High Performing Organization (HPO) review – the largest HPO review yet conducted at 554 FTE. As described in the Revised OMB Circular A-76, HPO reviews offer an alternative to conducting formal competitions with the private sector by applying the analytic rigor of an A-76 competition to an organization involving, in this case, civilian and military inherently governmental and commercial FTE.
- The Department submitted its 2006 Federal Activities Inventory Reform Act listing of commercial and inherently governmental FTE covering over 178,000 FTE. Over 77,000 of these FTE were listed by organization, function and location as performing commercial types of work (43 percent). Of the 77,000 DHS FTE listed as performing commercial work, in an agency that is largely oriented to law enforcement and federal disaster planning and recovery, 58,000 have been either exempted from competition by law or it has been found that in-house performance is required with related narrative justifications, by function and location. This inventory serves as baseline for determining the scope of the Department's competition requirements and for workforce planning.

**Improved Financial Performance** — accurately accounting for the taxpayers' money and giving managers timely and accurate program cost information to inform management decisions and control costs;

- Formalized the corrective action planning process through a Management Directive, guidance, and training.
- Implemented an automated corrective action tracking system to ensure progress is tracked and management is held accountable for progress.
- Developed a strategic planning process for improving financial management at DHS.
- Established ongoing reporting by the DHS OIG that assesses and compliments management's corrective action efforts through performance audits.

- Executed the first phase of our multi-year plan to implement a comprehensive internal control assessment pursuant to OMB A-123, Appendix A guidelines.
- The OCFO has developed a unified corrective action plan. This plan lists key milestones and completion dates for all financial statement material weaknesses through FY 2010.
- ICE has made measurable progress in implementing corrective actions which resulted in a reduction of its material weakness conditions.
- Initiated stand alone audits at FLETC. Continued stand alone audits at CBP and TSA.
- Established a financial policy working group. This group has completed an initial inventory of DHS financial management policies, constructed a matrix linking financial management policy and regulation, identified gaps, and prioritized the filling in of these gaps with a comprehensive set of financial management policies.

**Expanded Electronic Government** — ensuring that the Federal government investment in information technology significantly improves the government's ability to serve citizens, and that information technology systems are secure and delivered on time and on budget; and

- Developed and successfully implemented an Enterprise Architecture (EA) to guide investment decisions and systems development activities for the department. The use of the EA helps minimize unnecessary duplication of systems and also promotes appropriate intra- and inter-agency information sharing.
- Completed security certification and accreditation for 95 percent of the department's systems at the end of FY 2006, up from 35 percent at the beginning of the fiscal year.
- Complied with the FY 08 budget process requirement for identifying Federal Information Security Management Act (FISMA) systems that pertain to each major IT investment. Requiring that each FISMA system be mapped to an investment has resulted in a more accurate accounting for IT spending.
- Mapped all DHS IT investments to functional and IT portfolios, and developed portfolio cost reports. Supported the DHS CIO Council and Joint Requirements Council by conducting portfolio cost analyses.
- Implemented the cost/schedule/performance tracking of all major DHS investments on a quarterly basis. Developed a summary scorecard for each DHS component of quarterly cost/schedule/performance information for feedback to components and OMB eGov PMA reporting. Developed EVM guidance and training courses for DHS program management personnel.
- Achieved initial operating capability for DHS OneNet and for the DHS Stennis Data Center, thereby continuing to make progress in consolidating information technology (IT) infrastructure assets across the component agencies of DHS.
- Completed an interoperability baseline survey and version 2.0 of the statement of requirements for SAFECOM to improve interoperability for first responders.

**Budget and Performance Integration** — ensuring that performance is routinely considered in funding and management decisions and those programs achieve expected results and work toward continual improvement. For each initiative, the President's Management Agenda established clear, government-wide goals or standards for success.

- Completed the final 20% of Program Assessment Review Tool (PART) reviews of DHS mission area programs. DHS has now completed reviews of all of its major mission area programs. These PART reviews enabled programs to identify improvement areas and the development of actions plans to address them. Details of the PARTs completed during FY 2006 are found in the Program Evaluations section of this report.
- Utilized and demonstrated the marginal cost of incremental improvements in program performance metrics during budget formulation. Increased sophistication of performance budgeting included use of cost modeling of additional staffing. The ability to know and use the incremental cost of changes in program performance helps DHS become more efficient in accomplishing its mission.
- Provided better management information which couples program performance and management improvement of the President's Management Agenda with budget spending. This was accomplished by expanding the scope of component quarterly performance reporting to combine budget and performance information to enable quarterly reviews and assessments of progress in achieving annual targets in the annual performance plan and PART measures.
- Provided a DHS Congressional Budget Justification performance based budget in support of the President's Budget to Congress. The Performance Budget provided for each DHS program past and proposed funding, staffing levels, program goals and annual associated performance metrics in meeting the program goal. This combined information provides association of the level of program performance in outputs and results with funding levels for each program.

**Eliminating Improper Payments** – accurately identifying, preventing and eliminating erroneous payments.

- Completed statistically significant improper payments sample testing for Hurricane Katrina payments at FEMA. This testing identified FEMA's Disaster Relief Program as at high risk for improper payments (vendor and Individuals and Households Program [IHP] payments). FEMA management has begun recouping these improper payments and supplied a detailed corrective action plan which the Department is tracking.
- Completed an OMB Circular A-123 Management's Responsibility for Internal Control pilot of key internal controls over disbursements at FEMA. This pilot identified many areas for improvement which FEMA management is implementing.
- Completed statistically significant testing of all programs which issued more than \$100 million in FY 2005 disbursements at CBP, CIS, ICE, TSA, and USCG. Completed statistically significant testing of all programs which issued more than \$10 million in FY 2005 disbursements at FLETC and USSS. This testing did not identify any programs as at high risk for issuing improper payments but did lead to improvements in payment processing.
- Expanded recovery audit contract work to USCG. Continued recovery audit contract work at CBP and ICE.
- Improved the methodology for identifying Improper Payment Information Act (IPIA) programs.

**Real Property** – assuring that the Federal government's real property assets are available; of the right size and type; safe, secure and sustainable; able to provide quality workspaces; affordable; and operate efficiently and effectively.

- Developed the first accurate and current inventory of DHS real property assets. This inventory includes all installations, buildings, structures and land owned and operated in support of DHS missions. Inventory information is collected and maintained in accordance with Federal Real Property Council (FRPC) standards and was included in the first Government-wide real property database created in December 2005.
- Published the DHS Asset Management Plan which was approved in June 2006. This plan establishes the Department's goals and objectives to ensure that real property management is consistent with the DHS Strategic Plan, performance mea-

tures, and Federal Real Property Council (FRPC) standards.

- Established DHS-wide councils that provide management focus on real property across the Department and its components. The Chief Administrative Officer (CAO) Council and the Real Property Management Committee (RPMC) regularly convene to plan and manage the Department's real property program.

## LIMITATIONS OF THE FINANCIAL STATEMENTS

The principal financial statements have been prepared to report the financial position and results of operations of the entity, pursuant to the requirements of 31 U.S.C. 3515 (b). While the statements have been prepared from the books and records of the entity in accordance with GAAP for Federal entities and the formats prescribed by OMB, the statements are in addition to the financial reports used to monitor and control budgetary resources which are prepared from the same books and records.

The statements should be read with the realization that they are for a component of the U.S. Government, a sovereign entity.